在Catalyst 9800上使用錨點配置中央Web驗證

目錄

簡介

本檔案介紹如何在Catalyst 9800上設定和疑難排解中央Web驗證(CWA)，該驗證指向另一個無線LAN控制器(WLC)作為行動錨點，且使用AireOS或其他9800 WLC覆蓋目的地。

必要條件

需求

建議您瞭解9800 WLC、AireOS WLC和Cisco ISE的基本知識。假設在啟動CWA錨點設定之前，您

已經開啟了兩個WLC之間的行動通道。超出此組態範例的範圍。如需相關幫助，請參閱標題為「在Catalyst 9800控制器上建立行動通道」的文件

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

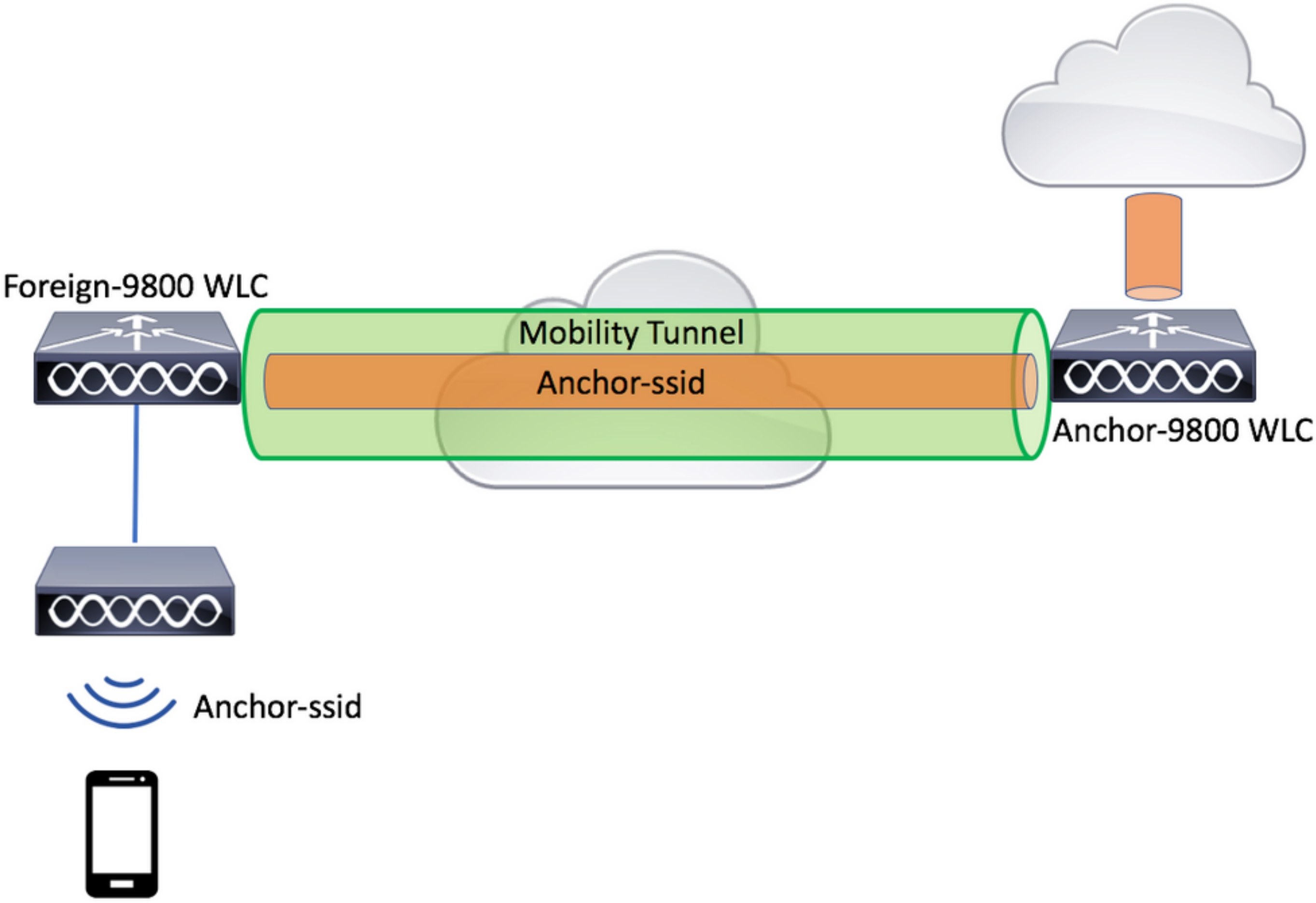
9800 17.2.1

5520 8.5.164 IRCM映像

ISE 2.4

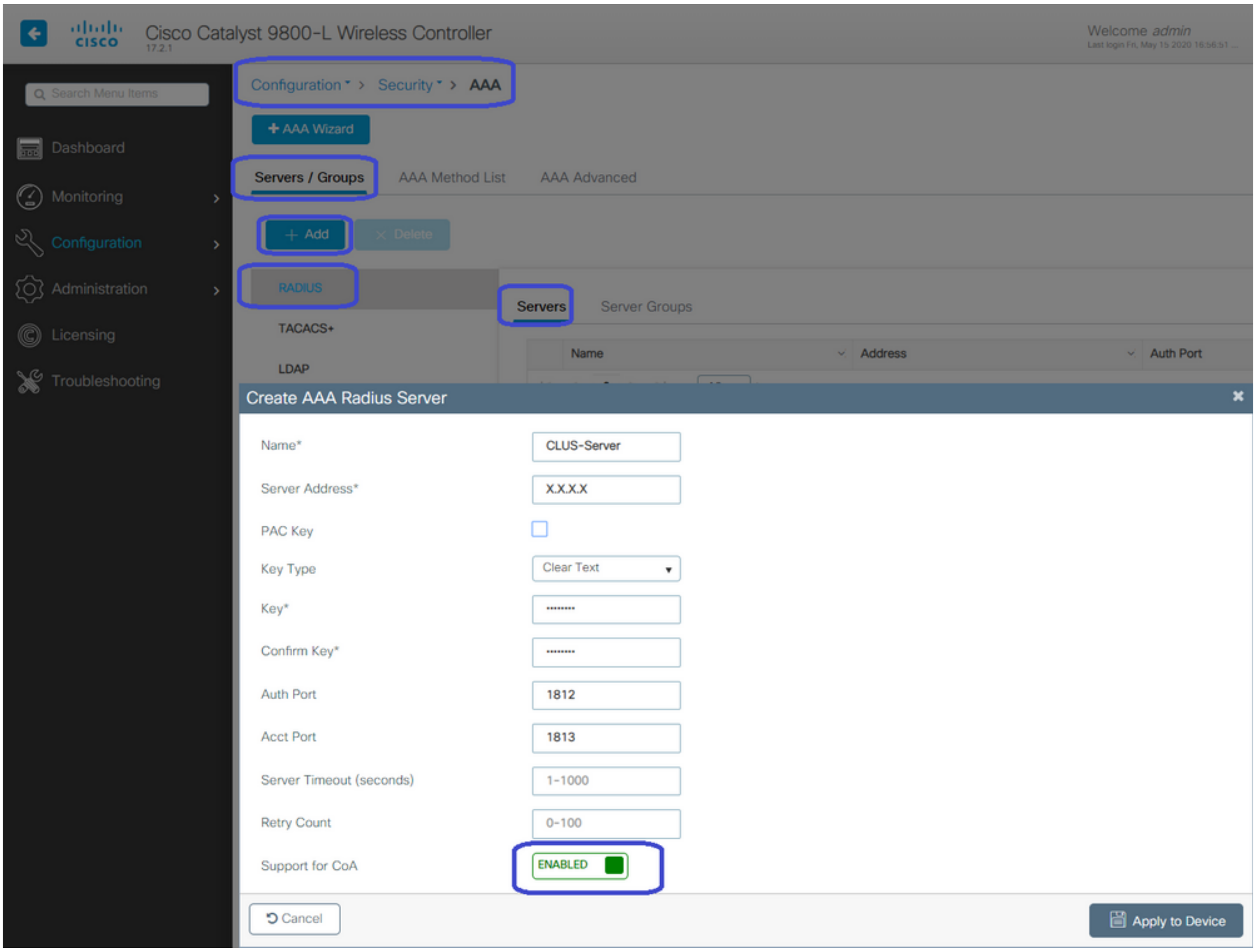
配置錨定到其他Catalyst 9800的Catalyst 9800

網路圖表



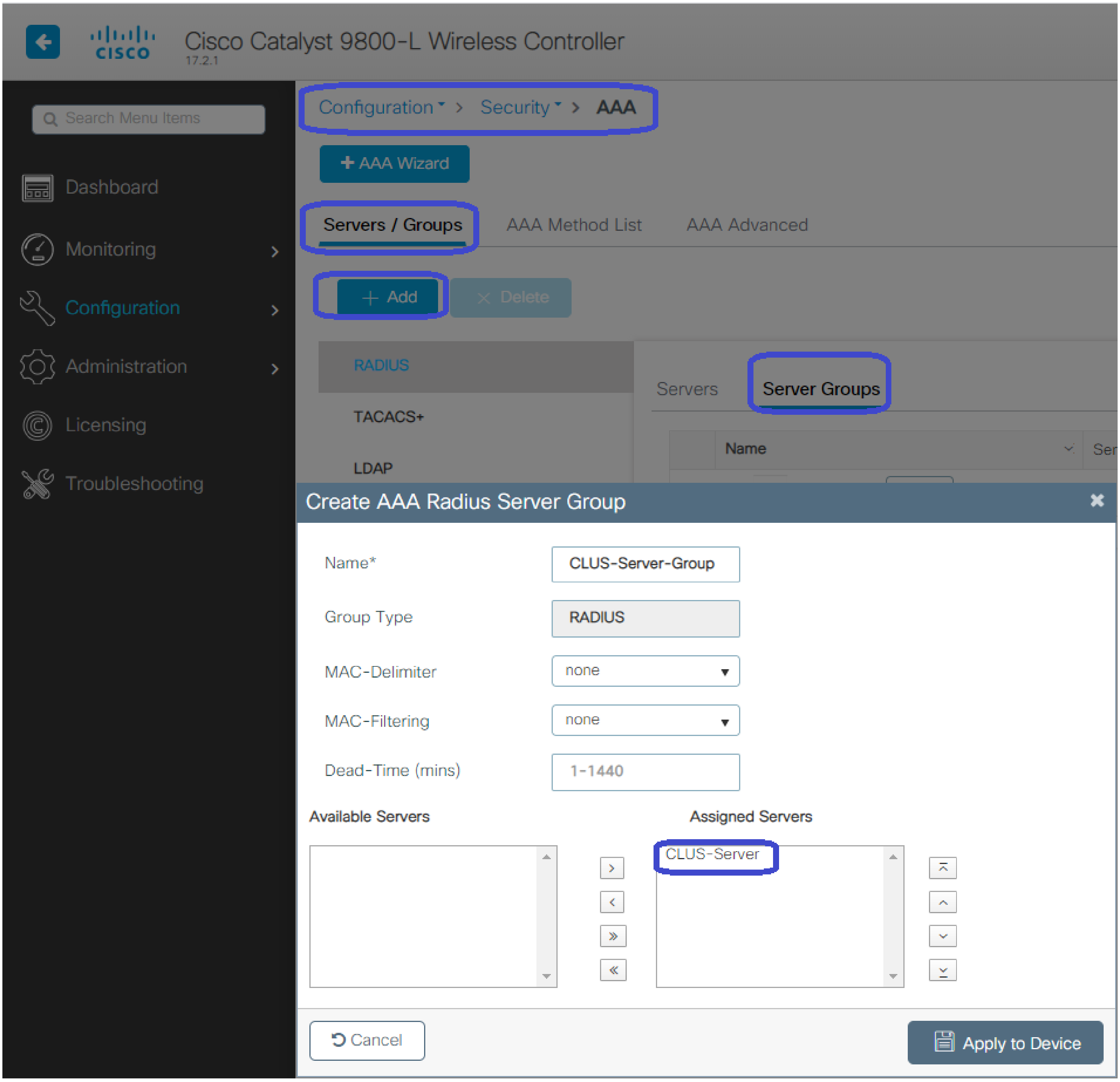
在兩台9800上配置AAA

在錨點和外部上，您需要先新增RADIUS伺服器並確保已啟用CoA。這可以在選單中完成
Configuration>Security>AAA>Servers/Groups>Servers>單擊Add按鈕



Name*	CLUS-Server
Server Address*	X.X.X.X
PAC Key	□
Key Type	Clear Text
Key*	········
Confirm Key*	········
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED

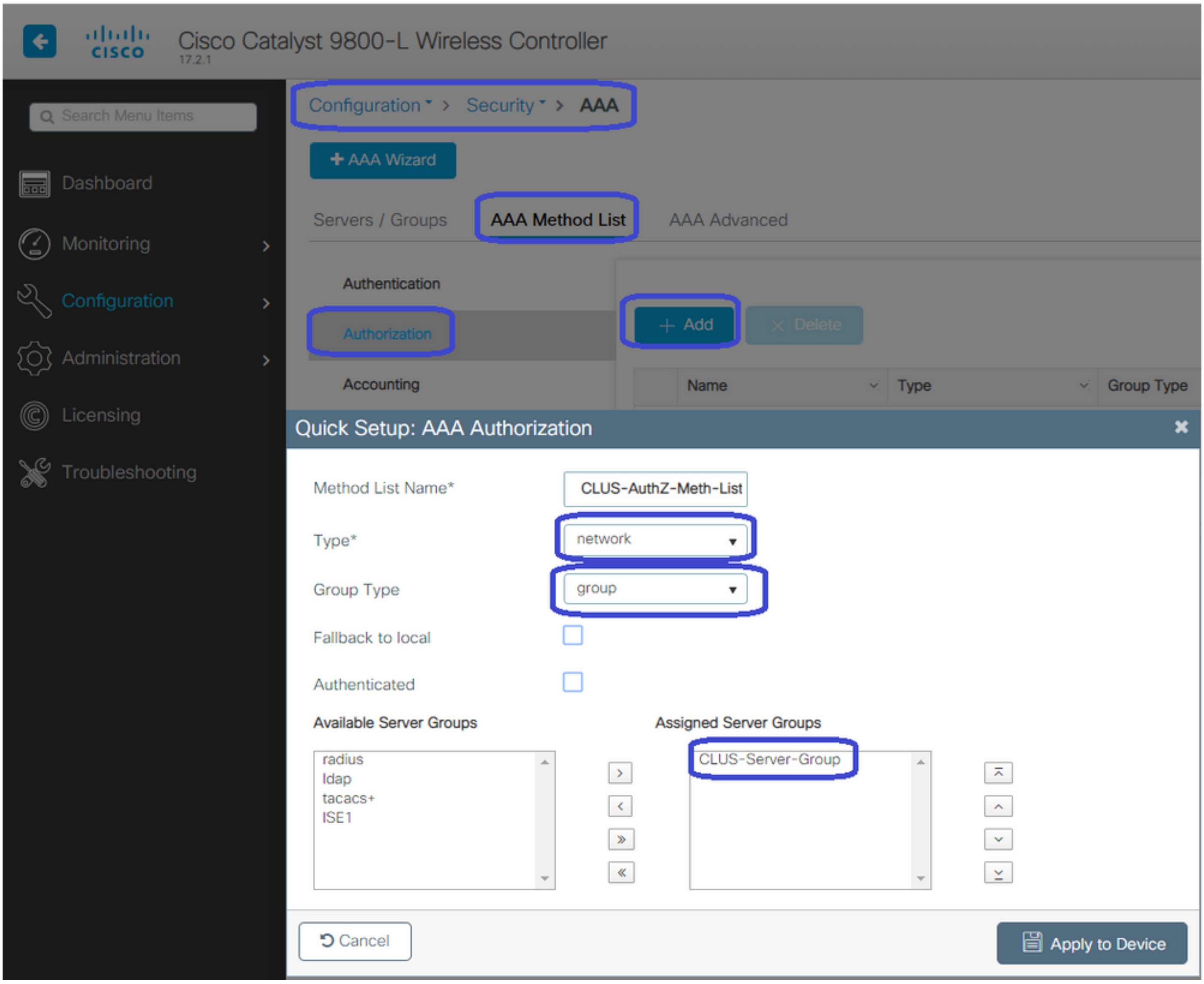
現在需要建立伺服器組，並將剛才配置的伺服器放入該組中。此操作在Configuration>Security>AAA>Servers/Groups>Server Groups>+Add處完成。



Name*	CLUS-Server-Group
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	1-1440

現在，建立一個authorization方法清單（對於CWA不需要身份驗證方法清單），其中型別為網路，組型別為組。將上一個操作中的伺服器組新增到此方法清單中。

此配置在此處完成Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add



Quick Setup: AAA Authorization

Method List Name*: CLUS-AuthZ-Meth-List

Type*: network

Group Type: group

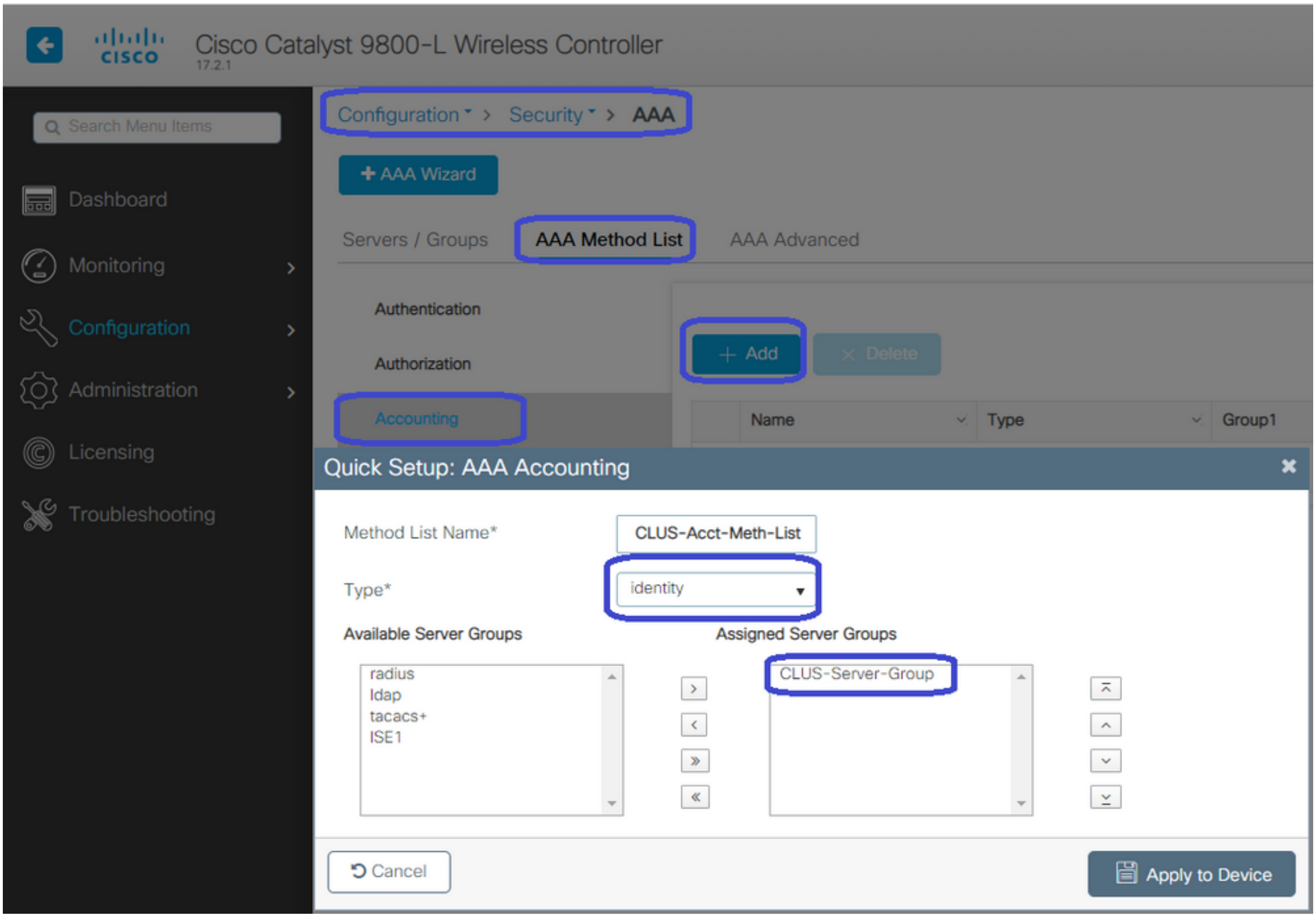
Fallback to local □

Authenticated □

Available Server Groups: radius, ldap, tacacs+, ISE1

Assigned Server Groups: CLUS-Server-Group

（可選）使用與授權方法清單相同的伺服器組建立記帳方法清單。可以在以下位置建立記帳清單 :Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add



Method List Name* CLUS-Acct-Meth-List

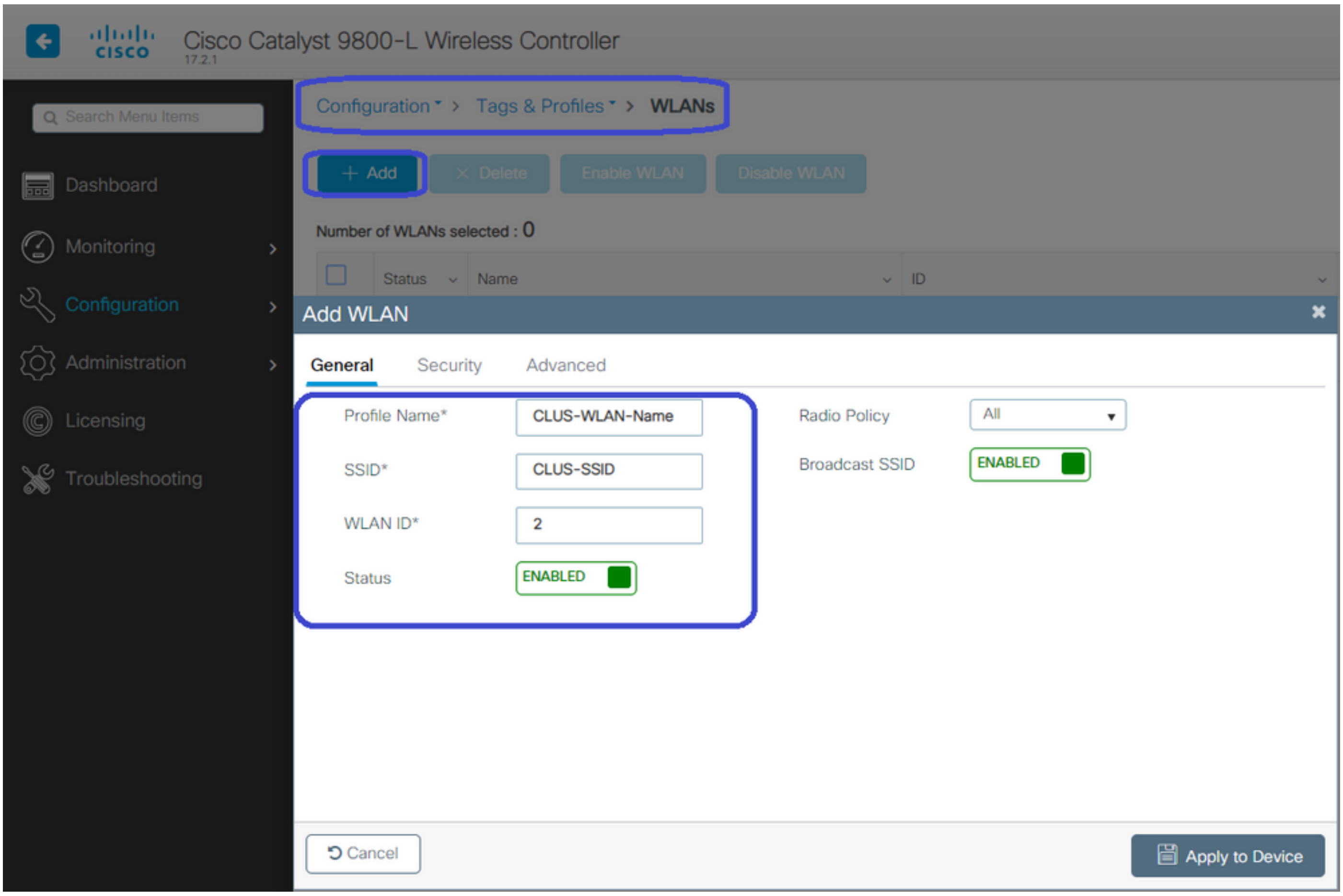
Type* identity

Available Server Groups: radius, ldap, tacacs+, ISE1

Assigned Server Groups: CLUS-Server-Group

在WLC上配置WLAN

在兩台WLC上建立和配置WLAN。兩者上的WLAN應該相符。安全型別應為mac過濾，並應應用上一步中的授權方法清單。此組態在**Configuration>Tags & Profiles>WLANs>+Add下完成**



Profile Name*: CLUS-WLAN-Name

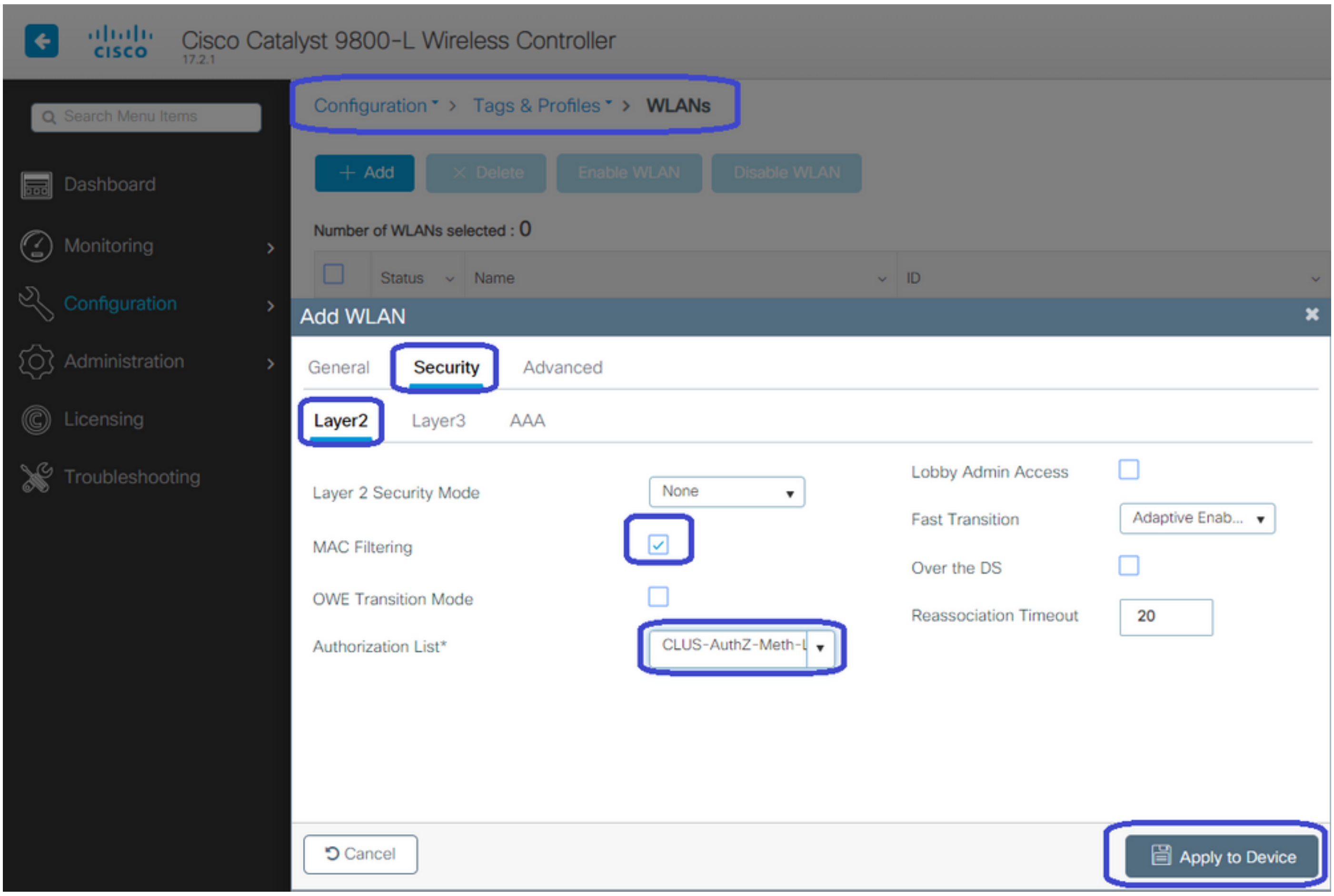
SSID*: CLUS-SSID

WLAN ID*: 2

Status: ENABLED

Radio Policy: All

Broadcast SSID: ENABLED



Layer 2 Security Mode: None

MAC Filtering: ☑

OWE Transition Mode: □

Authorization List*: CLUS-AuthZ-Meth-L

Lobby Admin Access: □

Fast Transition: Adaptive Enab...

Over the DS: □

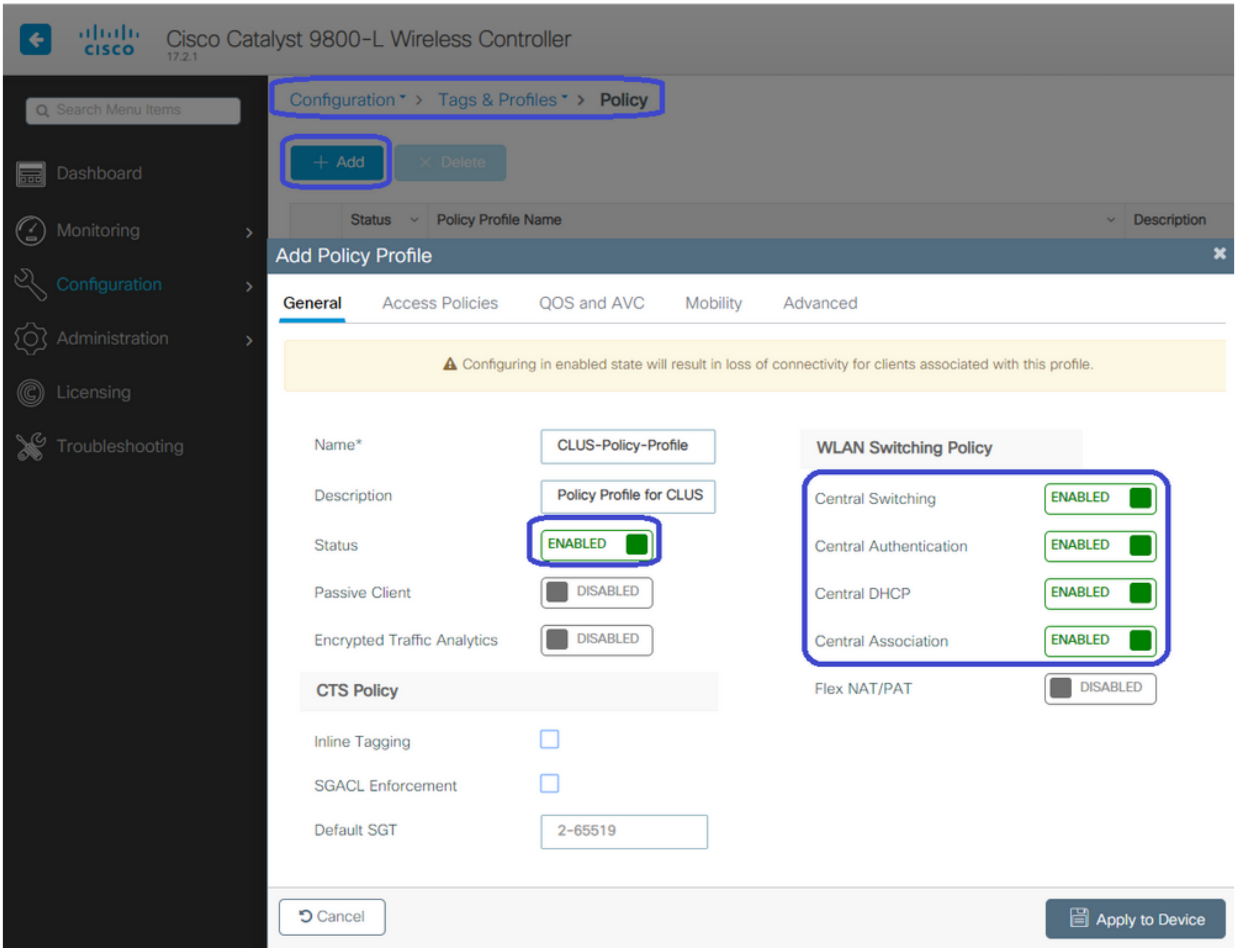
Reassociation Timeout: 20

在外部WLC上建立策略配置檔案和策略標籤

前往外部WLC Web UI。

要建立策略配置檔案，請轉到**配置>標籤和配置檔案>策略>+新增**

錨定時，必須使用中心交換。



⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name* CLUS-Policy-Profile

Description Policy Profile for CLUS

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging □

SGACL Enforcement □

Default SGT 2-65519

WLAN Switching Policy

Central Switching ENABLED

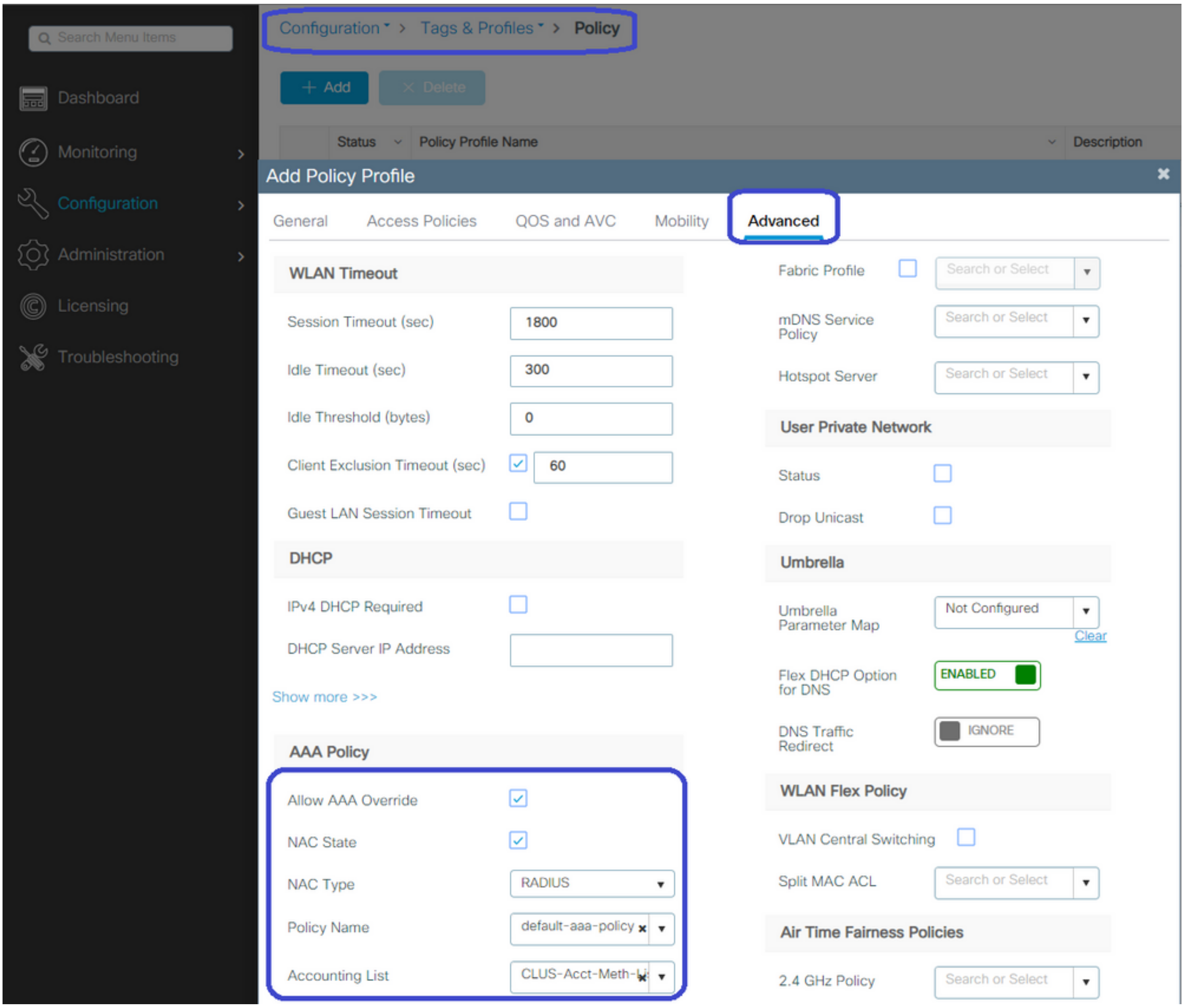
Central Authentication ENABLED

Central DHCP ENABLED

Central Association ENABLED

Flex NAT/PAT DISABLED

在「高級」頁籤上，CWA必須使用AAA覆蓋和RADIUS NAC。如果您選擇建立會計方法清單，還可以在此處應用該清單。



Add Policy Profile

WLAN Timeout

Session Timeout (sec) 1800

Idle Timeout (sec) 300

Idle Threshold (bytes) 0

Client Exclusion Timeout (sec) ☑ 60

Guest LAN Session Timeout □

DHCP

IPv4 DHCP Required □

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override ☑

NAC State ☑

NAC Type RADIUS

Policy Name default-aaa-policy

Accounting List CLUS-Acct-Meth-Li

Fabric Profile □ Search or Select

mDNS Service Policy Search or Select

Hotspot Server Search or Select

User Private Network

Status □

Drop Unicast □

Umbrella

Umbrella Parameter Map Not Configured Clear

Flex DHCP Option for DNS ENABLED

DNS Traffic Redirect IGNORE

WLAN Flex Policy

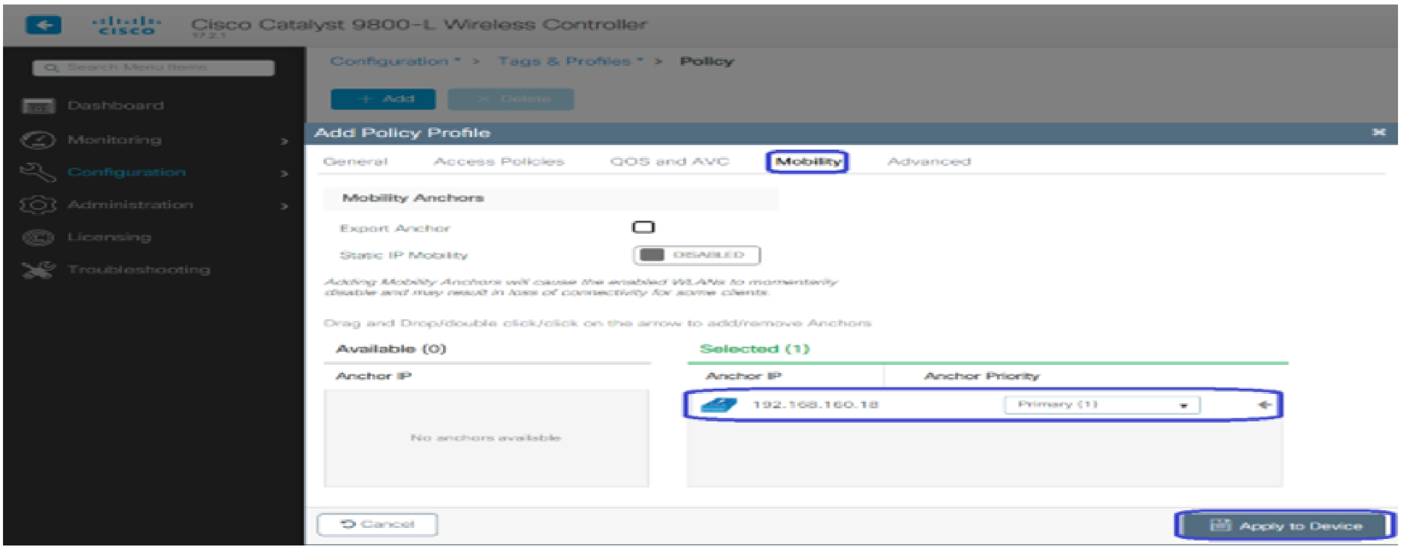
VLAN Central Switching □

Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

在「Mobility」索引標籤上，**請勿勾選「export anchor」覈取方塊，而是將錨點WLC新增到錨點清單中。**確保點選「應用到裝置」。 請注意，此假設兩個控制器之間已建立行動通道



Add Policy Profile

Mobility Anchors

Export Anchor □

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)

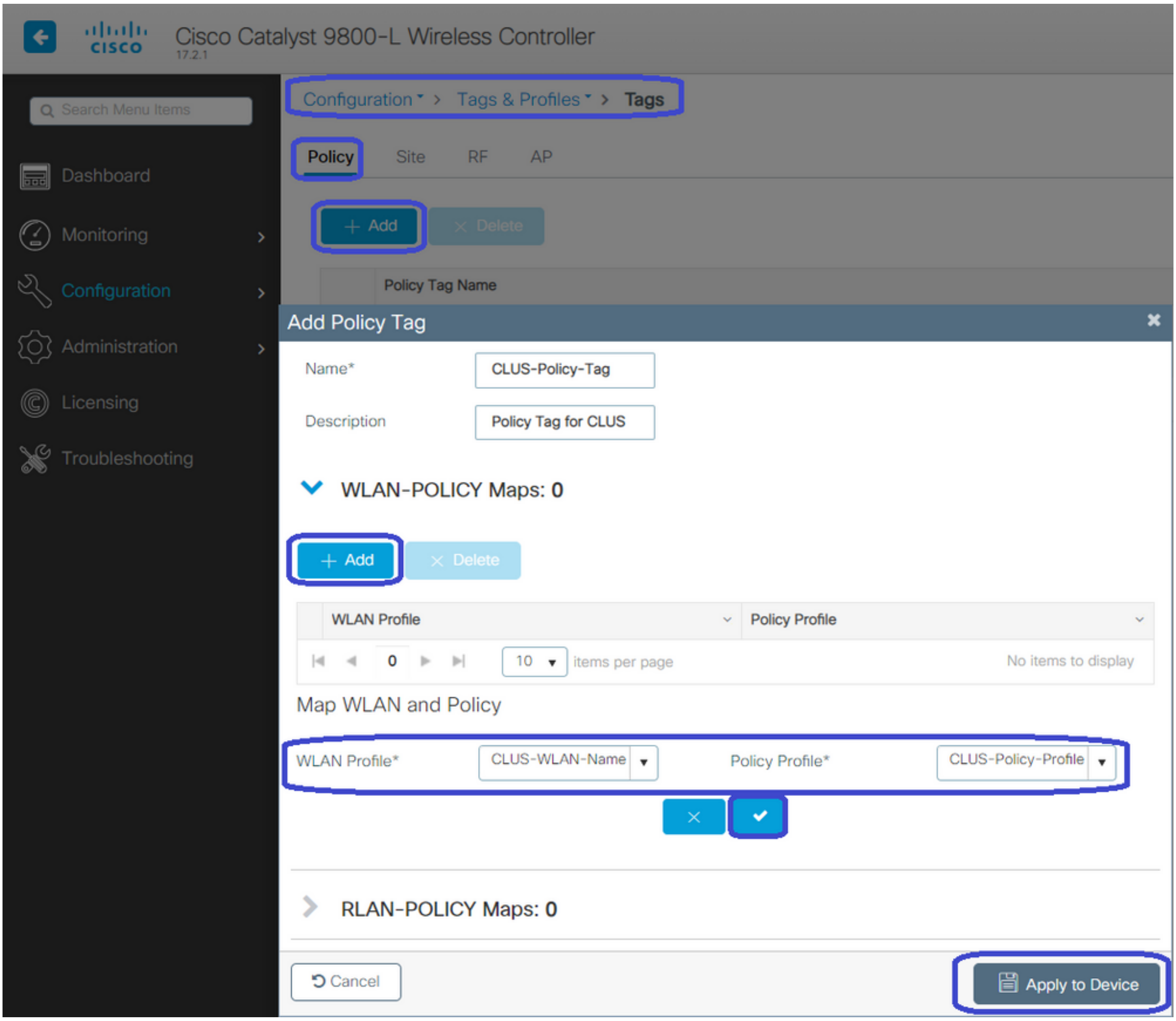
Anchor IP
No anchors available

Selected (1)

Anchor IP	Anchor Priority
192.168.160.18	Primary (1)

為了讓AP使用此策略配置檔案，您需要建立策略標籤並將其應用到要使用的AP。

要建立策略標籤，請轉至**Configuration>Tags & Profiles>Tags?Policy>+Add**



Add Policy Tag

Name* CLUS-Policy-Tag

Description Policy Tag for CLUS

WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile

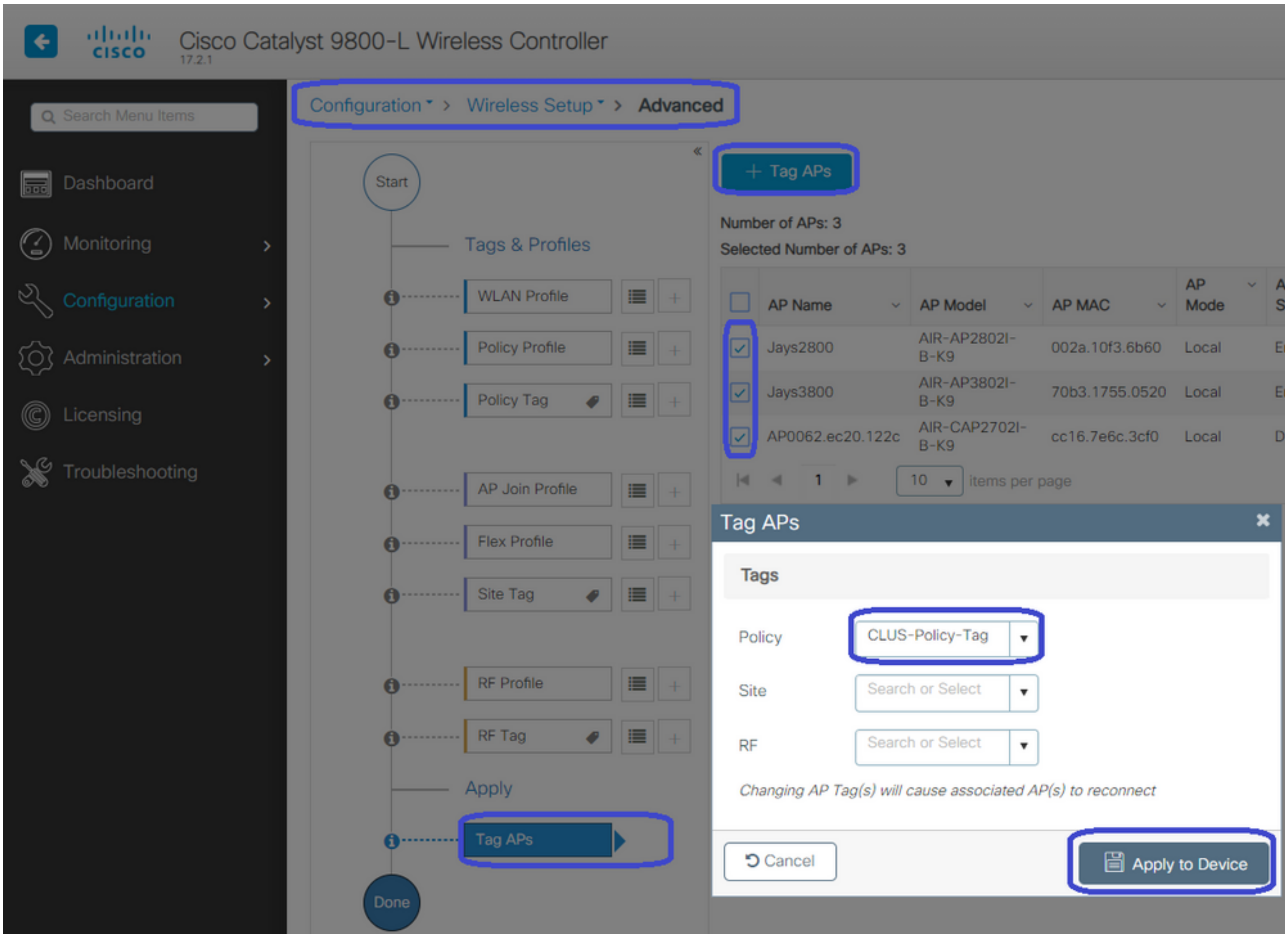
Map WLAN and Policy

WLAN Profile* CLUS-WLAN-Name

Policy Profile* CLUS-Policy-Profile

RLAN-POLICY Maps: 0

要同時將此項新增到多個AP，請轉到**配置>無線設定>高級>立即開始**。點選「標籤AP」旁邊的專案符號欄，將該標籤新增到您選擇的AP。



☐	AP Name	AP Model	AP MAC	AP Mode
☑	Jays2800	AIR-AP2802I-B-K9	002a.10f3.6b60	Local
☑	Jays3800	AIR-AP3802I-B-K9	70b3.1755.0520	Local
☑	AP0062.ec20.122c	AIR-CAP2702I-B-K9	cc16.7e6c.3cf0	Local

Policy: CLUS-Policy-Tag

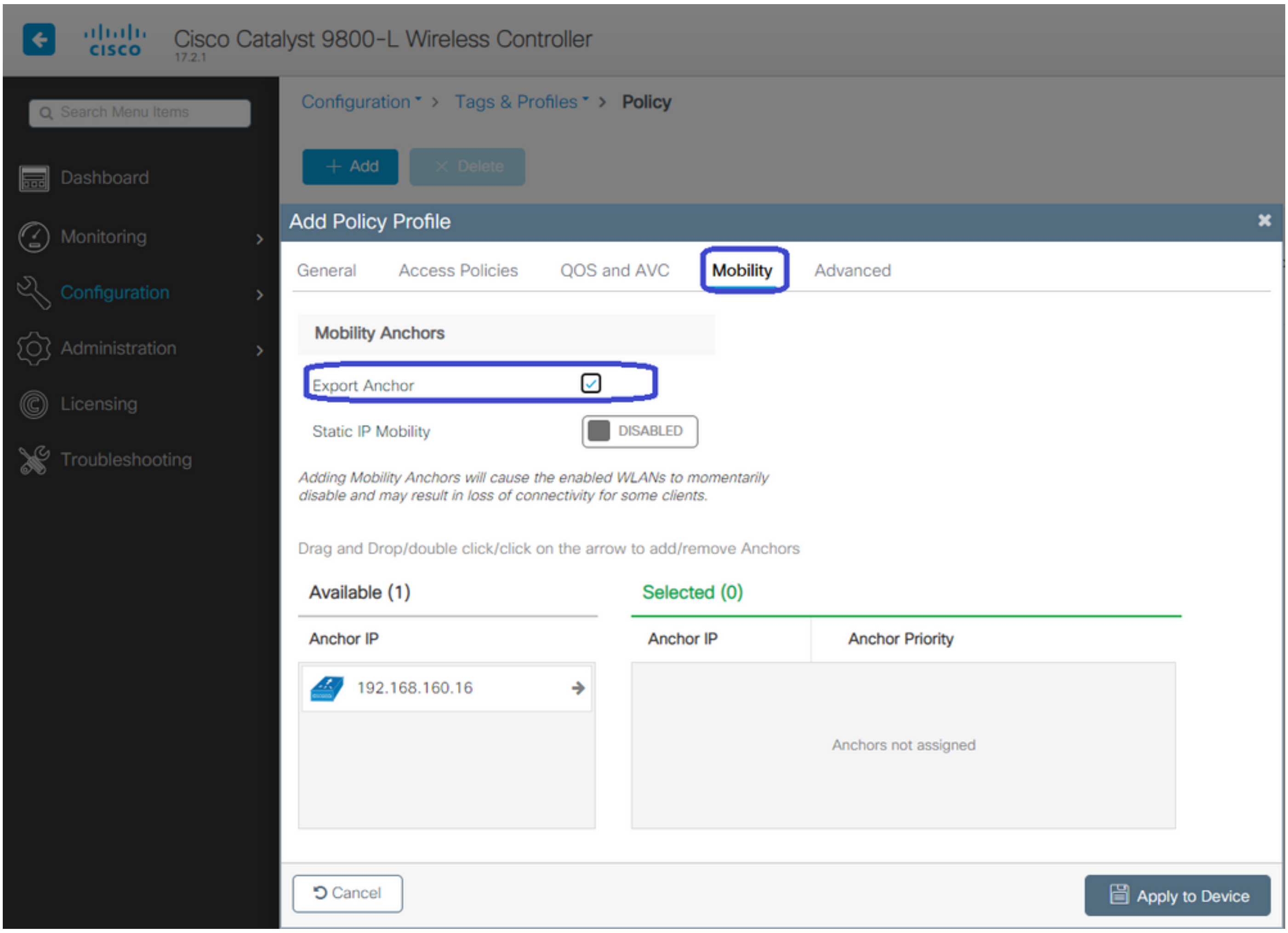
Changing AP Tag(s) will cause associated AP(s) to reconnect

在錨點WLC上建立策略配置檔案

前往錨點WLC Web UI。在錨點9800上**Configuration**>Tags & Profiles>**Tags>Policy>+Add下新增策略配置檔案**。確保此配置與外部裝置上的策略配置檔案相匹配，移動頁籤和記帳清單除外。

此處不新增錨點，但會勾選「匯出錨點」覈取方塊。請勿在此處新增記帳清單。請注意，此假設兩個控制器之間已建立行動通道

附註：沒有理由在策略標籤中將此配置檔案關聯到WLAN。如果您這樣做，將會出現問題。如果您想對此WLC上的AP使用相同的WLAN，請為其建立另一個原則設定檔。



Mobility Anchors

Export Anchor ☑

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)

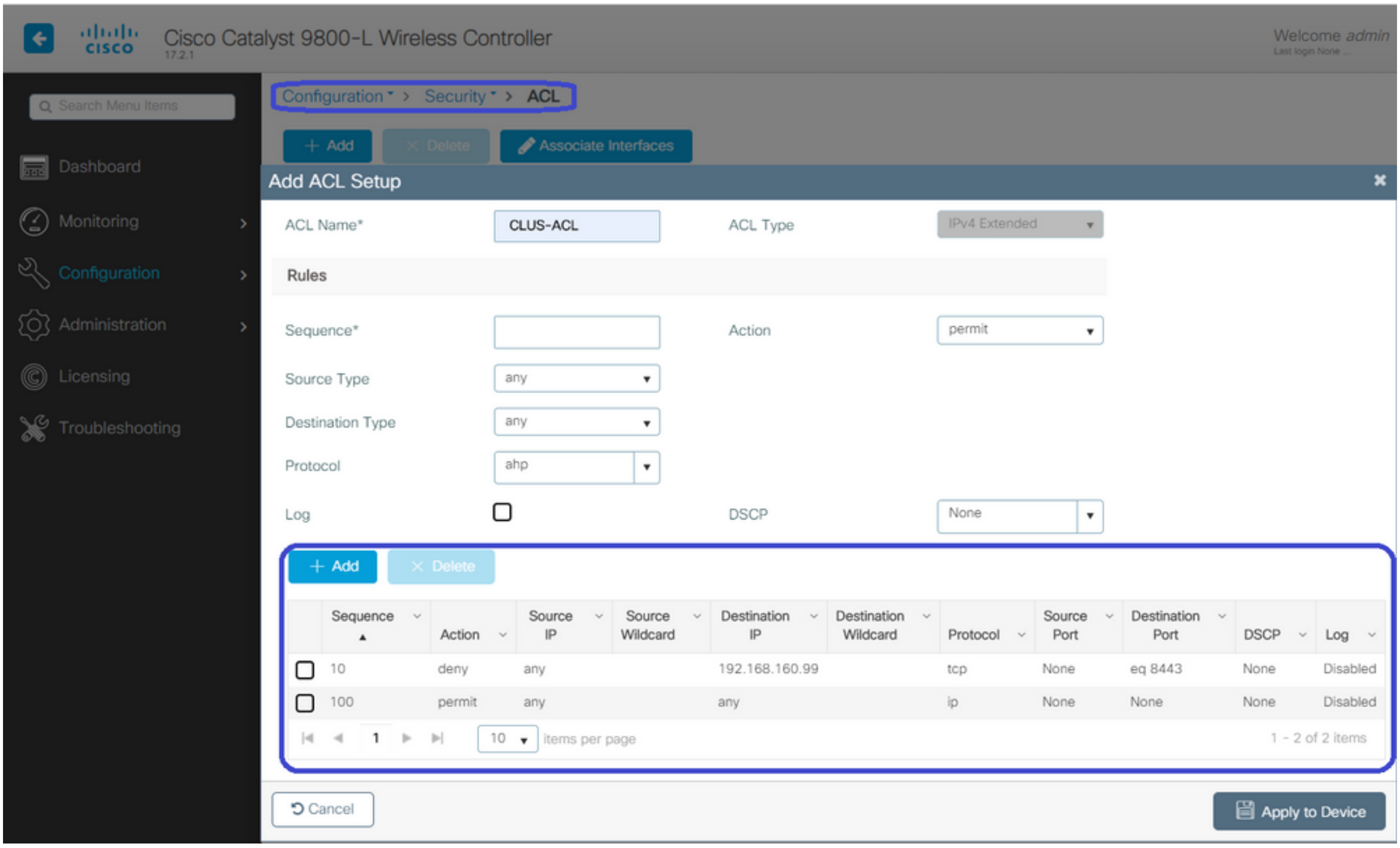
Anchor IP
192.168.160.16

Selected (0)

Anchor IP	Anchor Priority
Anchors not assigned	

重新導向兩台9800上的ACL設定

接下來，您需要在兩台9800上建立重新導向ACL組態。外部的條目並不重要，因為它是將ACL應用於流量的錨點WLC。唯一的要求是它在那裡，並且有一些條目。錨點上的條目必須「拒絕」埠8443上的ISE訪問，並且「允許」所有其他內容。此ACL僅適用於從客戶端「進入」的流量，因此不需要返回流量的規則。DHCP和DNS將在ACL中無條目的情況下通過。



ACL Name*	CLUS-ACL	ACL Type	IPv4 Extended
Sequence*		Action	permit
Source Type	any		
Destination Type	any		
Protocol	ahp		
Log	□	DSCP	None

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
□	10	deny	any		192.168.160.99		tcp	None	eq 8443	None	Disabled
□	100	permit	any		any		ip	None	None	None	Disabled

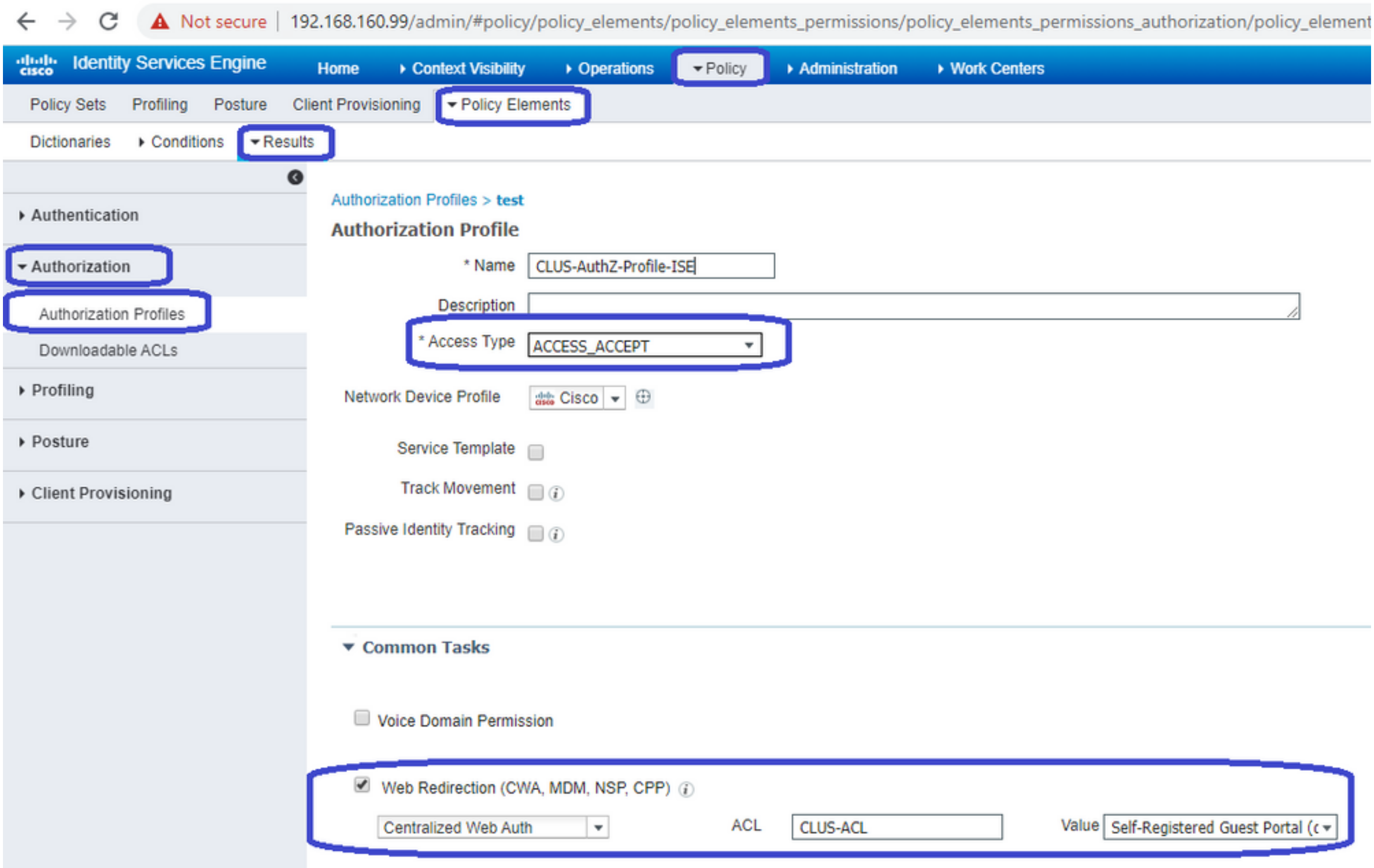
1 | 10 items per page | 1 - 2 of 2 items

配置ISE

最後一步是為CWA配置ISE。此方式有很多選項，但本示例將堅持基本並使用預設的自註冊訪客門戶。

在ISE上，您需要建立授權配置檔案、帶有身份驗證策略的策略集和使用授權配置檔案的授權策略，將9800（外部）作為網路裝置新增到ISE，並建立使用者名稱和密碼以登入網路。

要建立授權配置檔案，請轉至**Policy>Policy Elements>Authorization>Results>Authorization Profiles>**，然後按一下**Add**。確保返回的訪問型別為「access_accept」，然後設定要傳送回的AVP（屬性 — 值對）。對於CWA，重定向ACL和重定向URL是必需的，但您也可以傳送回諸如VLAN ID和會話超時等內容。非常重要，ACL名稱應與外部和錨點9800上的重新導向ACL名稱相匹配。



Authorization Profiles > test

Authorization Profile

* Name	CLUS-AuthZ-Profile-ISE
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Passive Identity Tracking	□

Common Tasks

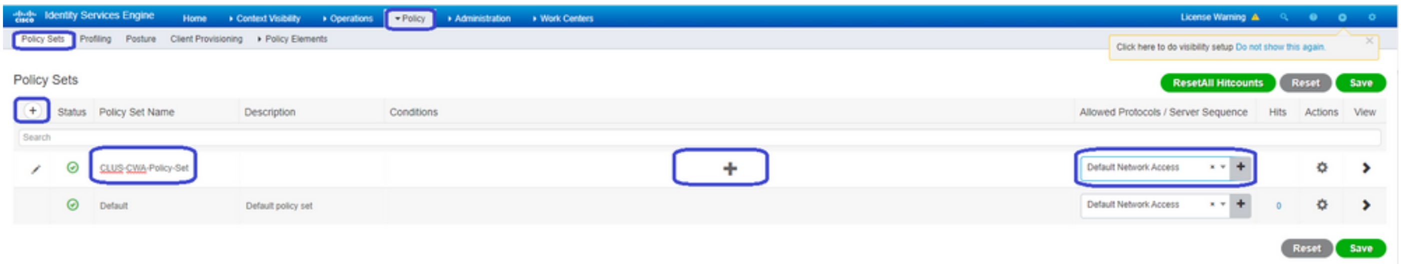
□ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth ACL CLUS-ACL Value Self-Registered Guest Portal (c

然後，您需要配置一種方法，將剛剛建立的授權配置檔案應用到通過CWA的客戶端。為此，一種方法是建立在使用MAB時繞過身份驗證的策略集，並在使用被叫站ID中傳送的SSID時應用授權配置檔案。同樣，有很多方法可以實現這一點，因此，如果您需要一些更具體或更安全的方法，這是最簡單的方法。

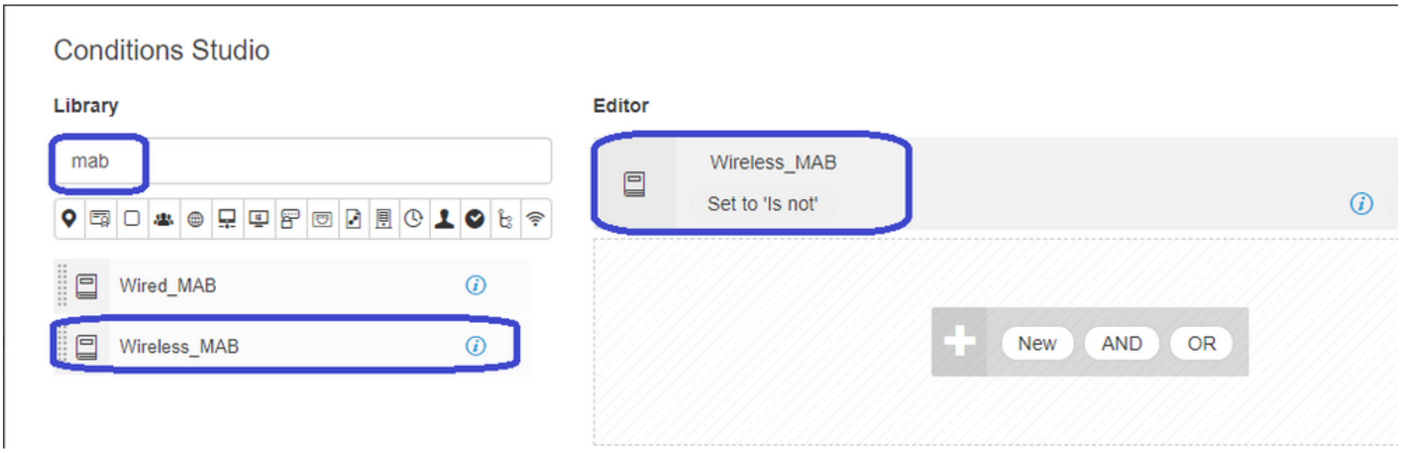
要建立策略集，請轉至**Policy>Policy Sets**，然後點選螢幕左側的+按鈕。命名新策略集，並確保將其設定為「預設網路訪問」或允許對MAB進行「進程主機查詢」的任何允許的協定清單（要檢查允許的協定清單，請轉至Policy>Policy Elements>Results>Authentication>Allowed Protocols）。 現在點選您建立的新策略集中間的+符號。



Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✓	CLUS-CWA-Policy-Set		+	Default Network Access		⚙	>
	✓	Default	Default policy set		Default Network Access	0	⚙	>

對於此策略設定，每次在ISE中使用MAB時，它將通過此策略設定。稍後，您可以制定與被叫站ID匹配的授權策略，以便根據使用的WLAN應用不同的結果。此流程非常可定製，可以匹配許多內容。



Conditions Studio

Library

mab

Wired_MAB

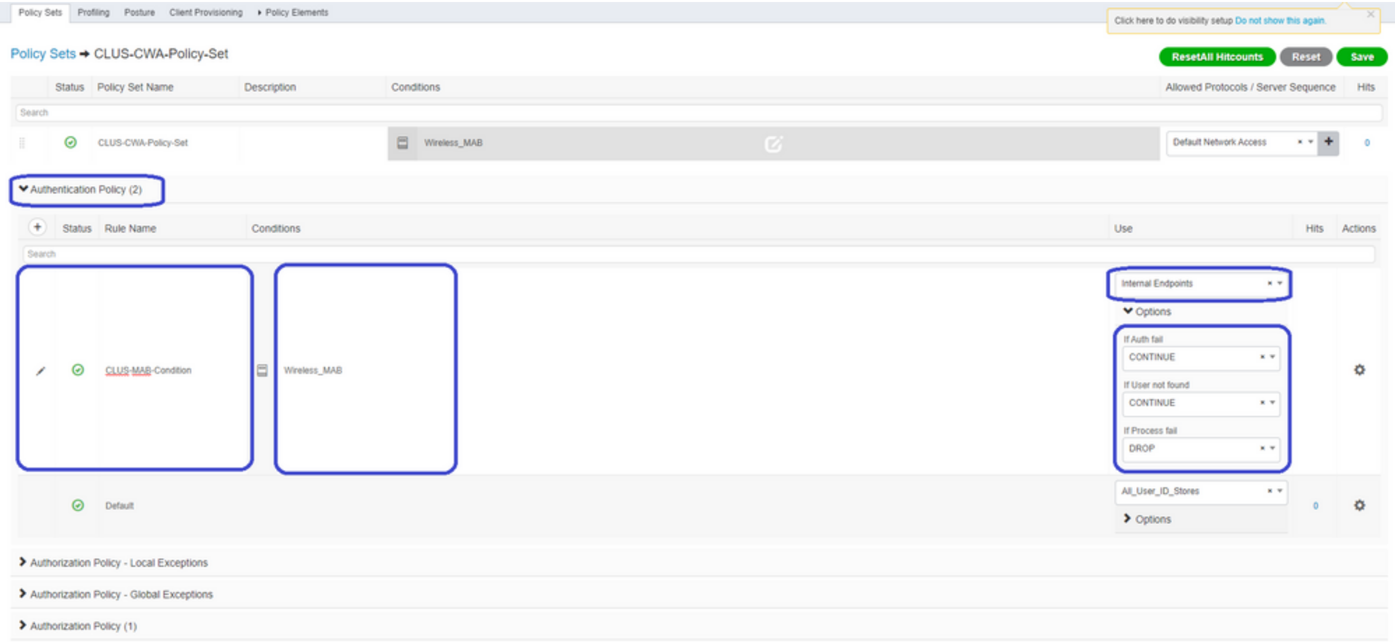
Wireless_MAB

Editor

Wireless_MAB

Set to 'Is not'

在策略集中，建立策略。身份驗證策略可以在MAB上再次匹配，但您需要更改ID儲存以使用「內部端點」，並且需要更改選項以繼續身份驗證失敗且找不到使用者。



Policy Sets → CLUS-CWA-Policy-Set

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access	0

Authentication Policy (2)

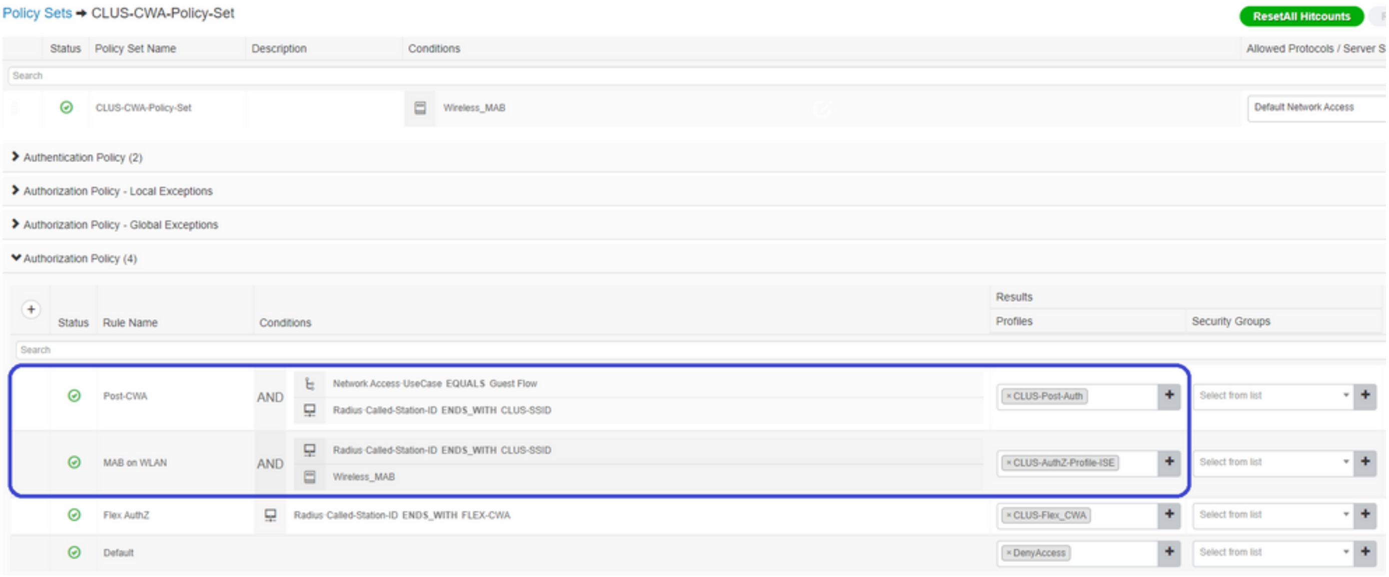
Status	Rule Name	Conditions	Use	Hits	Actions
✓	CLUS-MAB-Condition	Wireless_MAB	Internal Endpoints Options If Auth fail: CONTINUE If User not found: CONTINUE If Process fail: DROP		⚙
✓	Default		All_User_ID_Stores Options	0	⚙

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

設定身份驗證策略後，需要在授權策略中建立兩個規則。此策略看上去像ACL，因此順序需要將post-auth規則放在頂部，將pre-auth規則放在底部。後身份驗證規則將匹配已通過訪客流的使用者。也就是說，如果他們已經登入，他們將遵循該規則並停止。如果他們尚未登入，則會繼續下清單並點選獲取重定向的預身份驗證規則。最好將授權策略規則與以SSID結尾的被叫站ID相匹配，以便僅對配置為這樣做的WLAN進行命中。



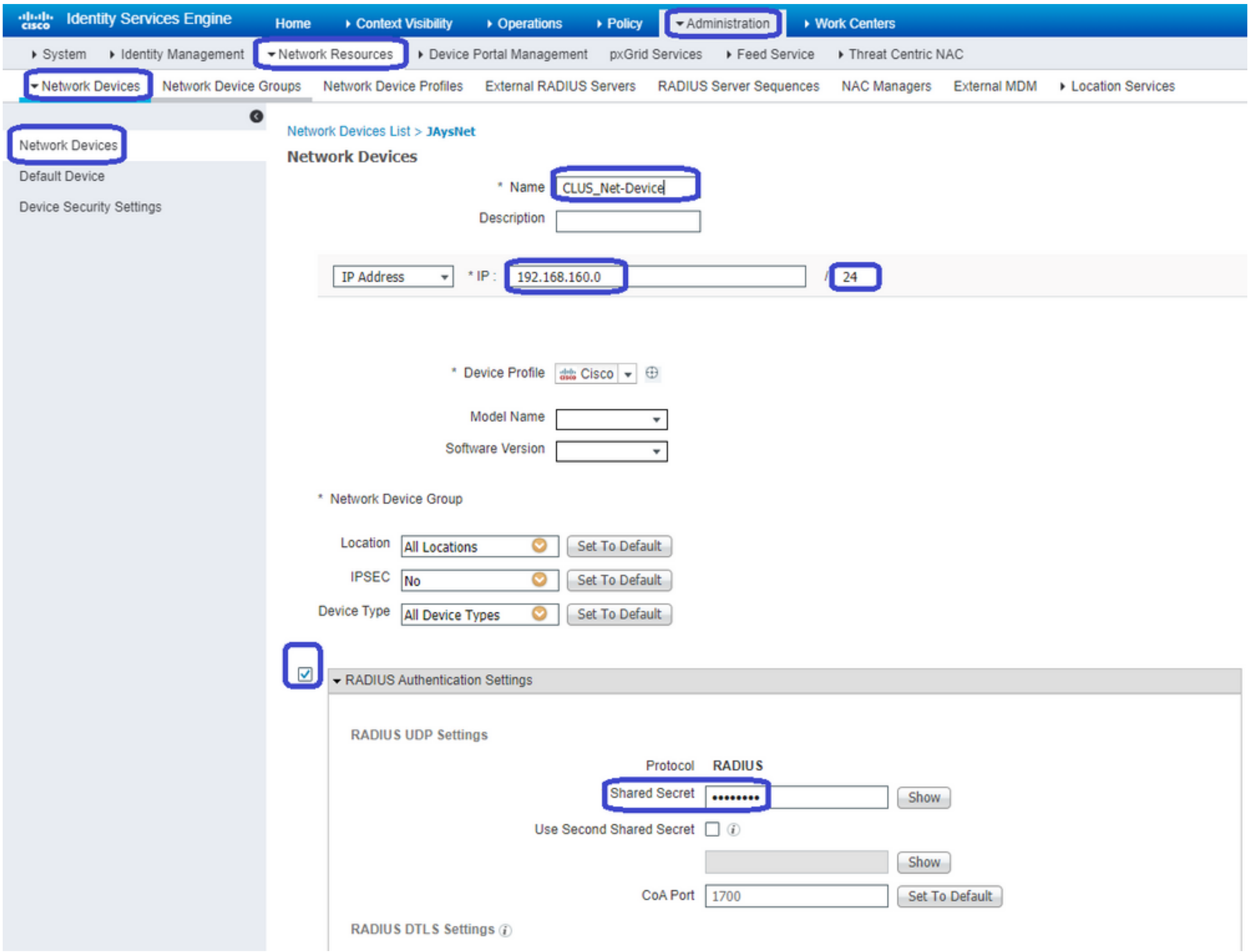
Policy Sets ➡ CLUS-CWA-Policy-Set

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

- Authentication Policy (2)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (4)

Status	Rule Name		Conditions	Results: Profiles	Security Groups
✓	Post-CWA	AND	Network Access·UseCase EQUALS Guest Flow Radius·Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth	Select from list
✓	MAB on WLAN	AND	Radius·Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE	Select from list
✓	Flex AuthZ		Radius·Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA	Select from list
✓	Default			DenyAccess	Select from list

現在策略集已配置，您需要通知ISE關於9800（外部），以便ISE將其信任為身份驗證器。這可以在**Admin>Network Resources>Network Device>+中執**行。您需要為其命名、設定IP地址（在本例中為整個管理子網）、啟用RADIUS並設定共用金鑰。ISE上的共用金鑰必須與9800上的共用金鑰匹配，否則此進程將失敗。新增配置後，按一下「提交」按鈕儲存配置。



Network Devices

* Name: CLUS_Net-Device

Description:

IP Address ▾ * IP : 192.168.160.0 / 24

* Device Profile: Cisco ▾

Model Name: ▾

Software Version: ▾

* Network Device Group

Location	All Locations	Set To Default
IPSEC	No	Set To Default
Device Type	All Device Types	Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: •••••••• Show

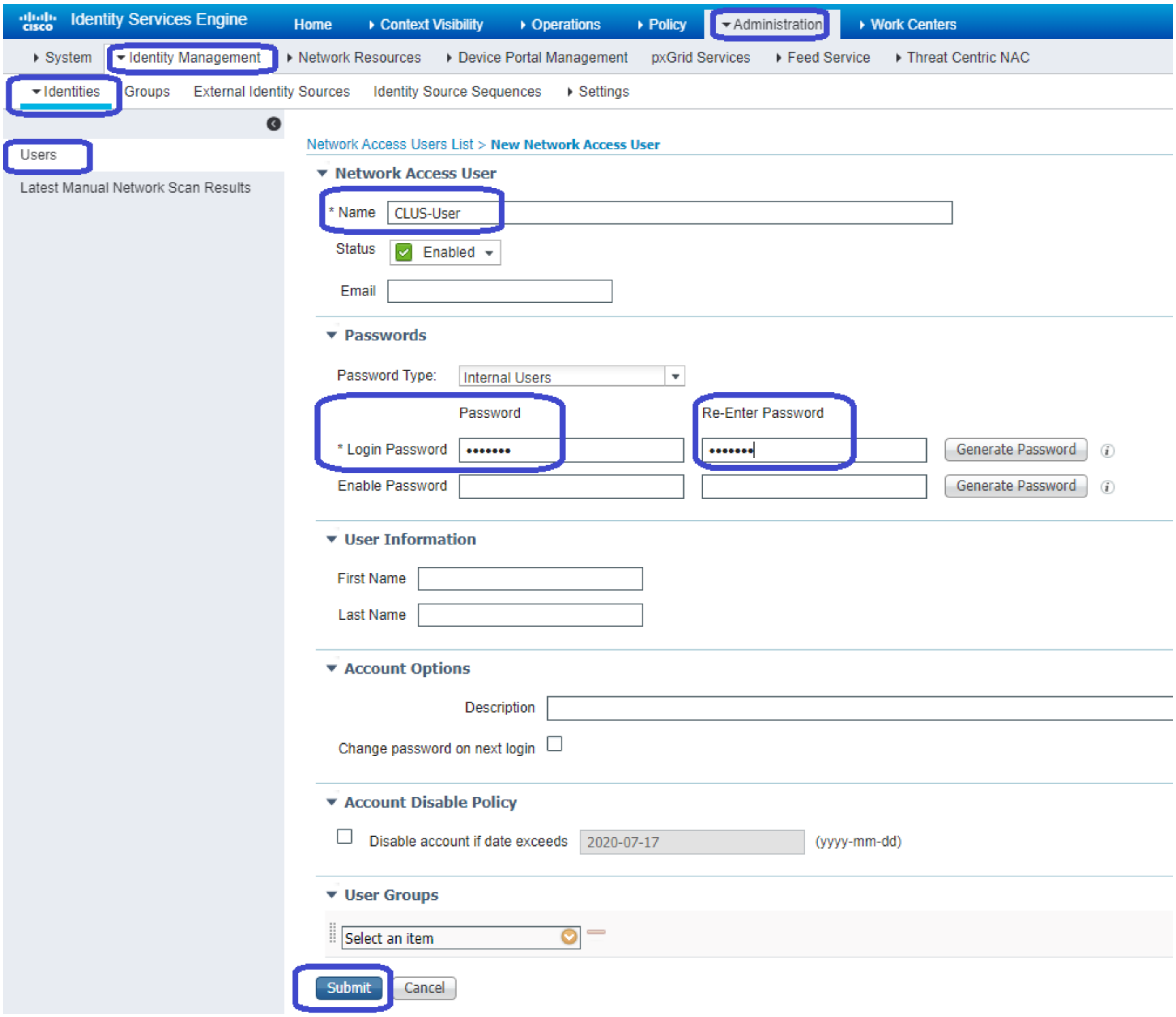
Use Second Shared Secret □

Show

CoA Port: 1700 Set To Default

RADIUS DTLS Settings

最後，您需要將客戶端要輸入的使用者名稱和密碼新增到登入頁面，以驗證他們是否有權訪問網路。此操作在**Admin>Identity Management>Identity>Users>+Add**下完成，並確保在新增後按submit。 與ISE的所有其他配置一樣，這是可自定義的，無需使用者本地儲存，但也是最簡單的配置。



Network Access Users List > **New Network Access User**

Network Access User

* Name: CLUS-User

Status: ☑ Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	•••••••	•••••••
Enable Password		

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

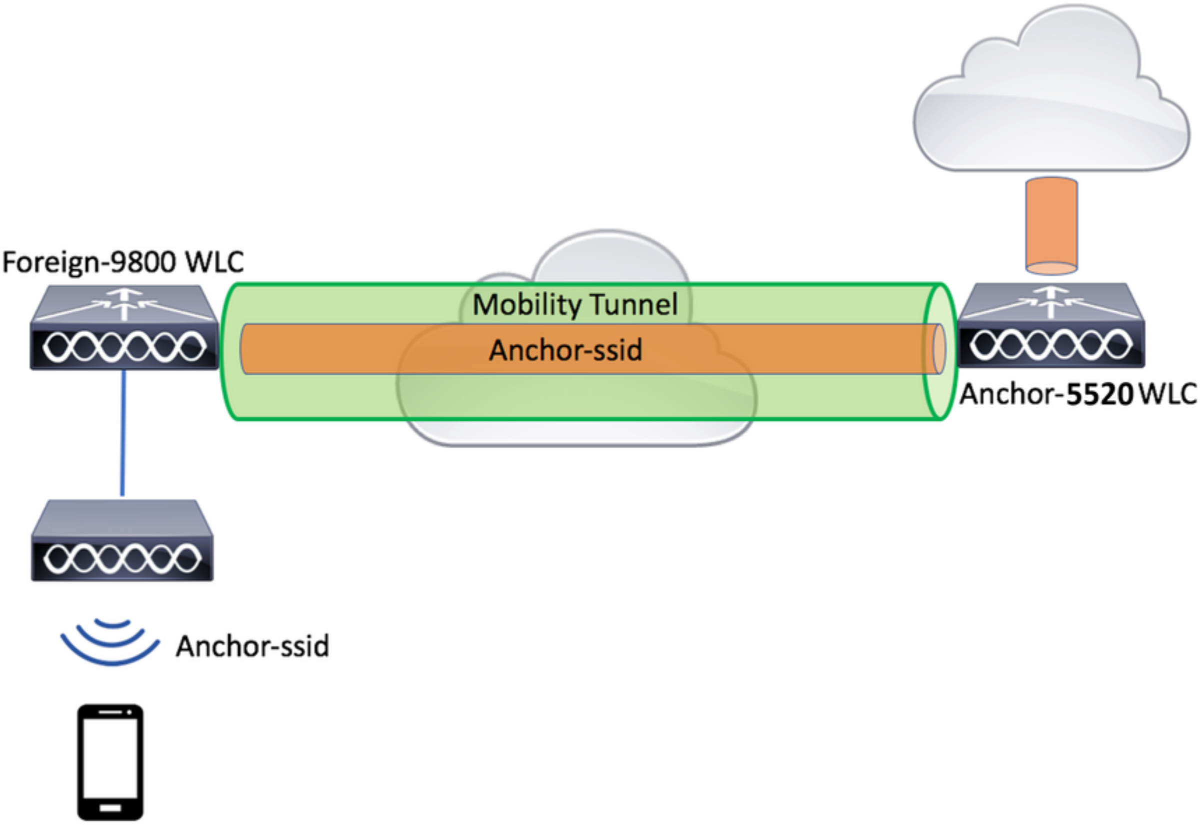
Account Disable Policy

□ Disable account if date exceeds 2020-07-17 (yyyy-mm-dd)

User Groups

Select an item

設定錨點到AireOS WLC的Catalyst 9800

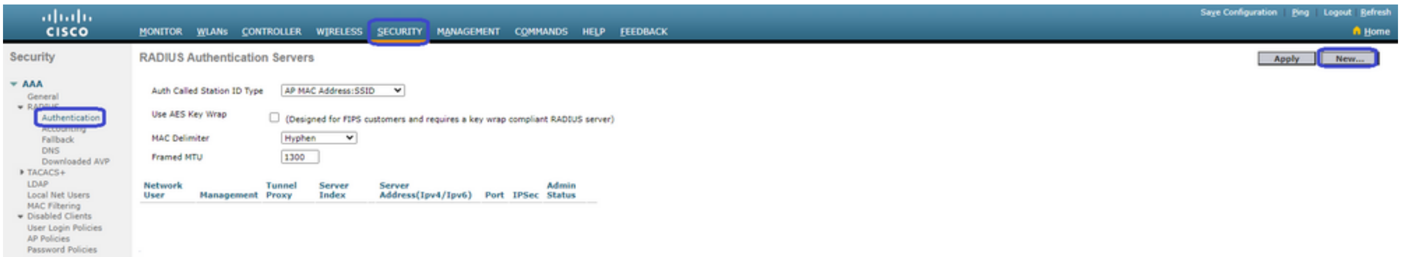


Catalyst 9800外部配置

按照前面討論的步驟操作，跳過「在錨*點WLC上建立策略配置檔案*」部分。

錨點AireOS WLC上的AAA配置

前往**Security>AAA>RADIUS>Authentication>New**，將伺服器新增到WLC。新增伺服器IP地址、共用金鑰和支援CoA。



RADIUS Authentication Servers

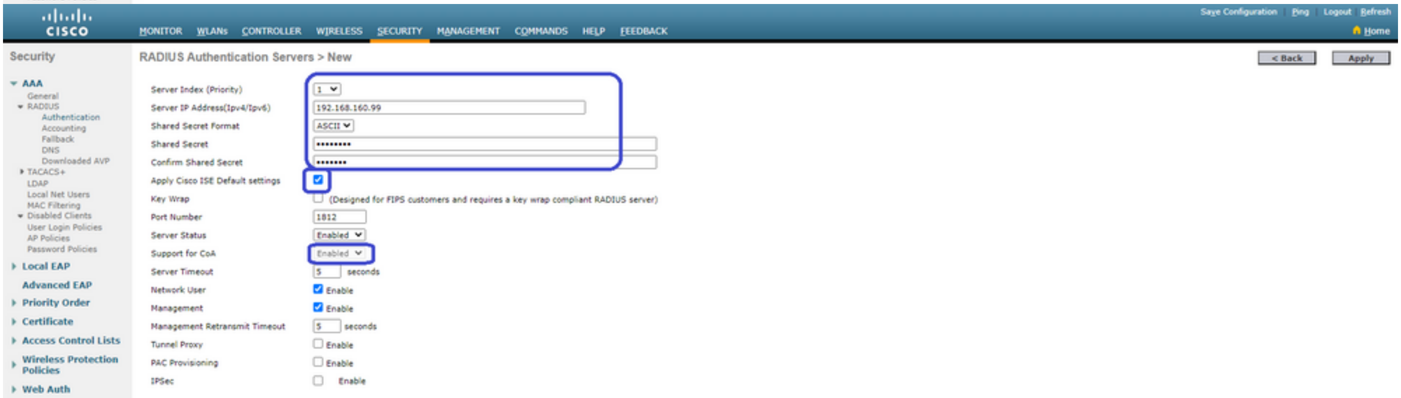
Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status



RADIUS Authentication Servers > New

Server Index (Priority): 1

Server IP Address(Ipv4/Ipv6): 192.168.160.99

Shared Secret Format: ASCII

Shared Secret: •••••••••

Confirm Shared Secret: ••••••••

Apply Cisco ISE Default settings: ☑

Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for CoA: Enabled

Server Timeout: 5 seconds

Network User: ☑ Enable

Management: ☑ Enable

Management Retransmit Timeout: 5 seconds

Tunnel Proxy: □ Enable

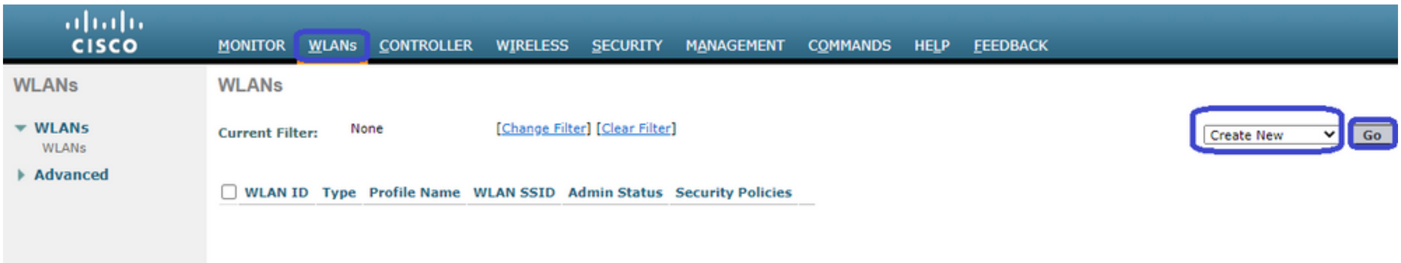
PAC Provisioning: □ Enable

IPSec: □ Enable

AireOS WLC上的WLAN配置

若要建立WLAN，請轉至**WLANs>Create New>Go**。

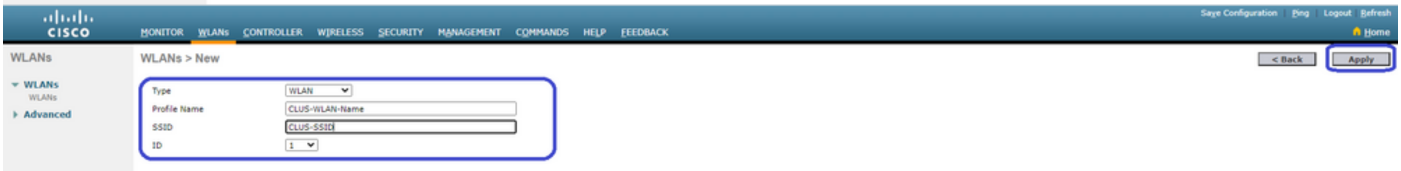
配置配置檔名稱、WLAN ID和SSID，然後點選「Apply」。


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
Advanced
Create New
Go

WLANs

Current Filter: None [Change Filter] [Clear Filter]

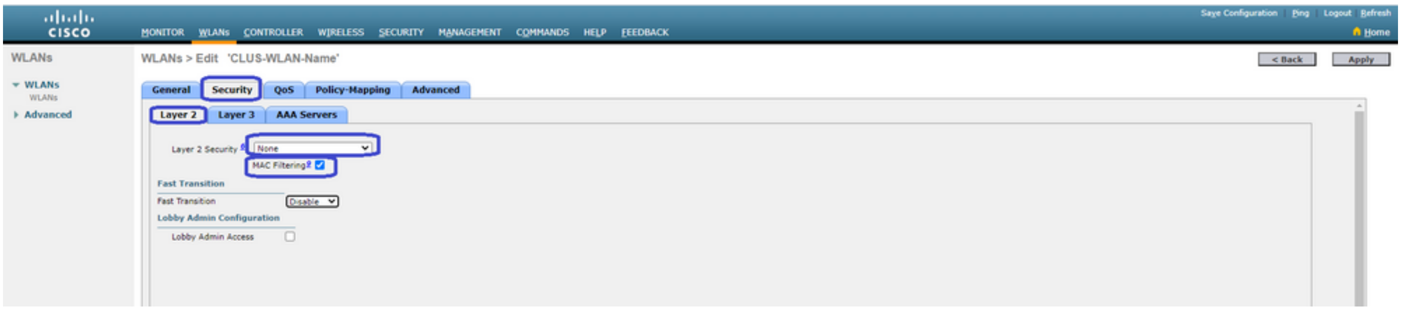
□ WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
< Back
Apply

WLANs > New

Type: WLAN
Profile Name: CLUS-WLAN-Name
SSID: CLUS-SSID
ID: 1

這麼做應會進入無線區域網組態。在「General」頁籤上，如果您不打算配置ISE在AVP中傳送，您可以新增希望客戶端使用的介面。接下來，前往**Security>Layer2**索引標籤，並匹配在9800上使用的「Layer 2 Security」配置並啟用「MAC Filtering」。


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
< Back
Apply
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers

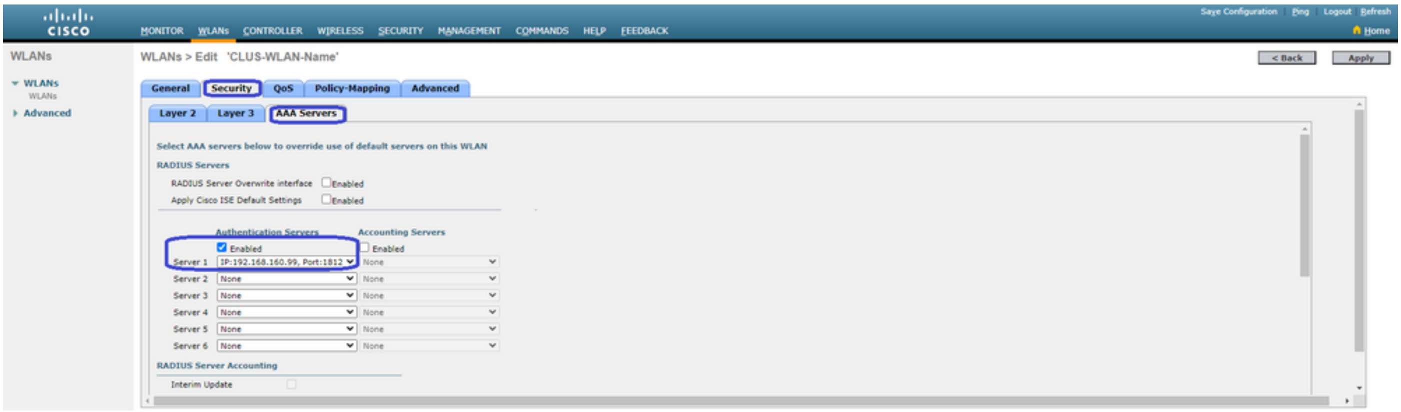
WLANs > Edit 'CLUS-WLAN-Name'

Layer 2 Security: None
MAC Filtering ☑

Fast Transition
Fast Transition: Disable

Lobby Admin Configuration
Lobby Admin Access □

現在移至**Security>AAA Servers**頁籤，並將ISE伺服器設定為「Authentication Servers」。 **請勿為**「記帳伺服器」設定任何內容。 取消選中「啟用」框以進行記帳。


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
< Back
Apply
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers

WLANs > Edit 'CLUS-WLAN-Name'

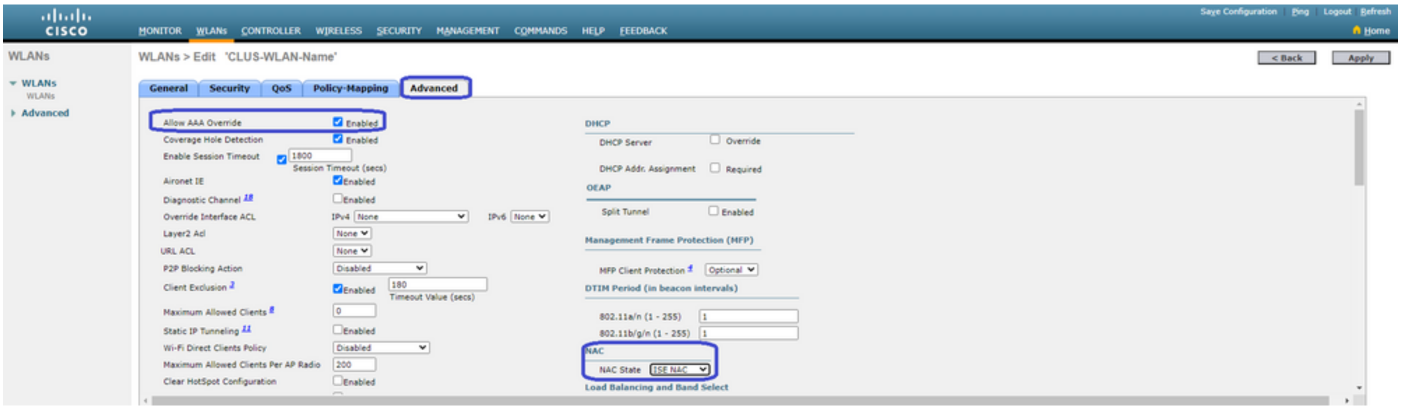
Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers
RADIUS Server Overwrite interface □Enabled
Apply Cisco ISE Default Settings □Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	□ Enabled
Server 1	IP:192.168.160.99, Port:1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

RADIUS Server Accounting
Interim Update □

仍處於WLAN配置中時，移至「Advanced」頁籤並啟用「Allow AAA Override」，並將「NAC State」更改為「ISE NAC」



WLANs > Edit 'CLUS-WLAN-Name'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑Enabled
Diagnostic Channel [18] □Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion [3] ☑Enabled 180 Timeout Value (secs)
Maximum Allowed Clients [8] 0
Static IP Tunneling [11] □Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration □Enabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel □ Enabled

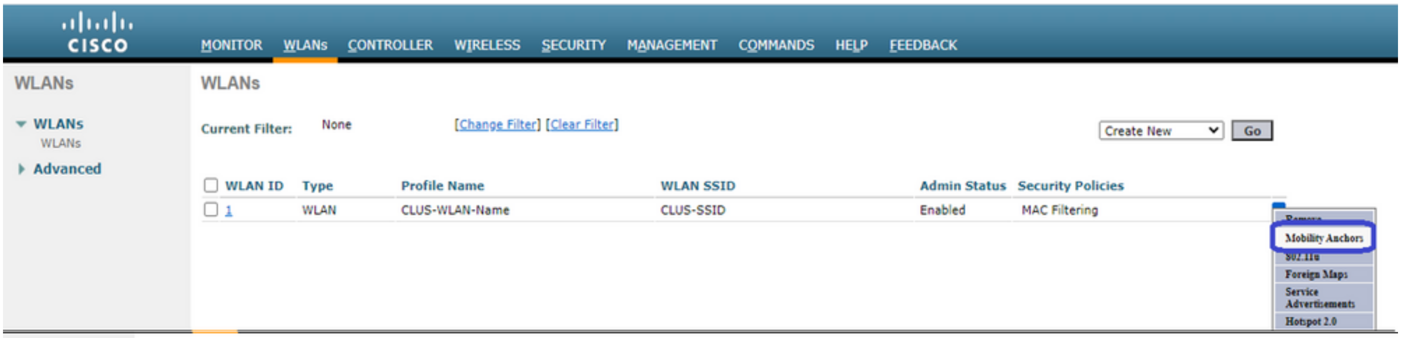
Management Frame Protection (MFP)
MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State ISE NAC

Load Balancing and Band Select

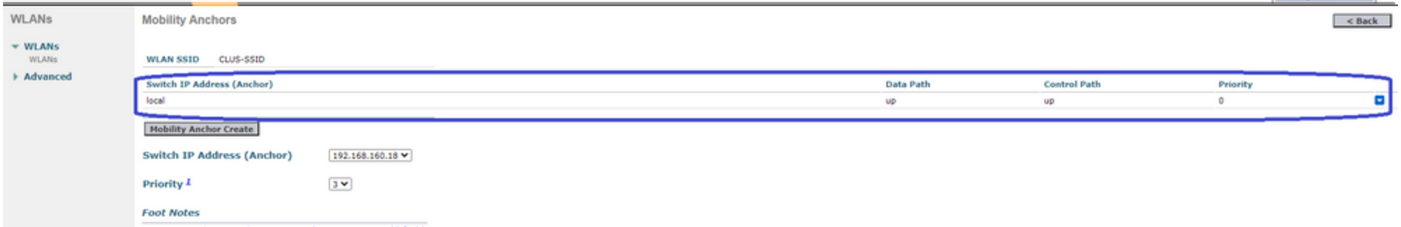
最後是把它固定在自己身上。若要執行此操作，請返回**WLANs**頁面，並懸停在WLAN>移動錨點右側的藍色框上。將「Switch IP Address(Anchor)(交換機IP地址（錨點）)」設定為「local」，然後按下「Mobility Anchor Create」按鈕。隨後應顯示優先順序0為本地錨點。



WLANs

Current Filter: None

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	CLUS-WLAN-Name	CLUS-SSID	Enabled	MAC Filtering



Mobility Anchors

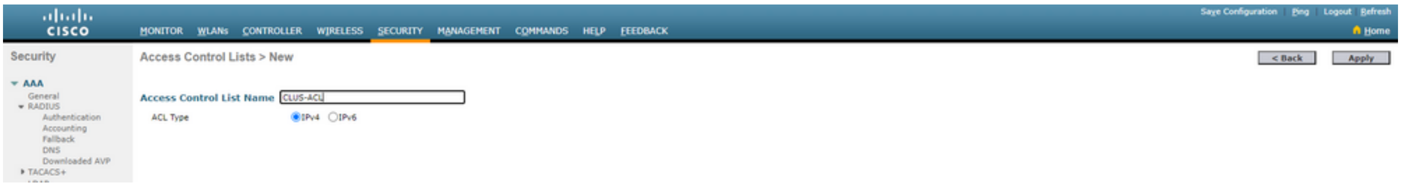
WLAN SSID CLUS-SSID

Switch IP Address (Anchor)	Data Path	Control Path	Priority
local	up	up	0

Switch IP Address (Anchor) 192.168.160.18
Priority [1] 3

在AireOS WLC上重定向ACL

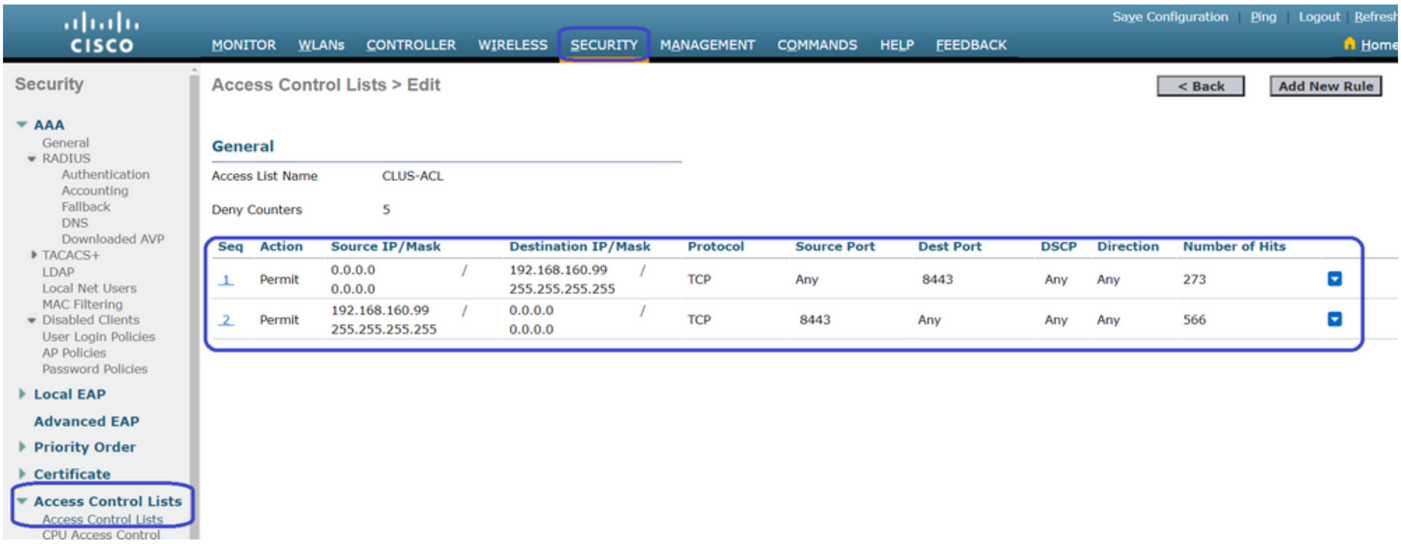
這是AireOS WLC上所需的最終配置。若要建立重新導向ACL，請前往**Security>Access Control Lists>Access Control Lists>New**。輸入ACL名稱（該名稱必須與AVP中傳送的名稱匹配），然後點選「Apply」。



Access Control Lists > New

Access Control List Name CLUS-ACL
ACL Type ● IPv4 ○ IPv6

現在，按一下剛建立的ACL的名稱。按一下「新增新規則」按鈕。與AireOS WLC上的9800控制器不同，您可以為允許到達ISE的流量配置允許語句，而無需重定向。 預設情況下允許DHCP和DNS。



Access Control Lists > Edit

General

Access List Name CLUS-ACL

Deny Counters 5

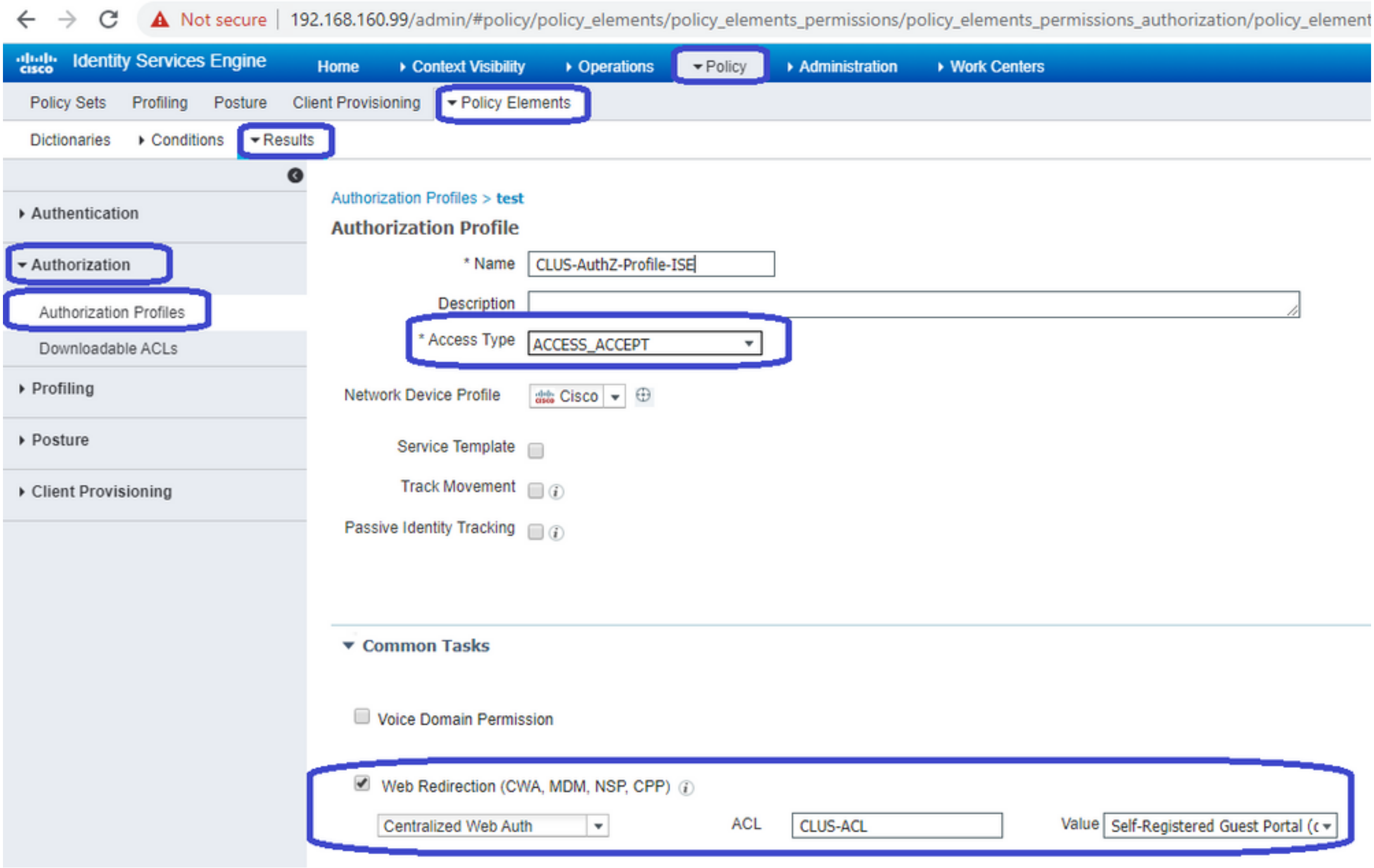
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	192.168.160.99 / 255.255.255.255	TCP	Any	8443	Any	Any	273
2	Permit	192.168.160.99 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	566

配置ISE

CWAISE

ISE9800ISE

Policy>Policy Elements>Authorization>Results>Authorization Profiles>+Addaccess_acceptAVP — CWAACLURLVLAN ID ACLWLCWLCACL



Authorization Profiles > test

Authorization Profile

* Name CLUS-AuthZ-Profile-ISE

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

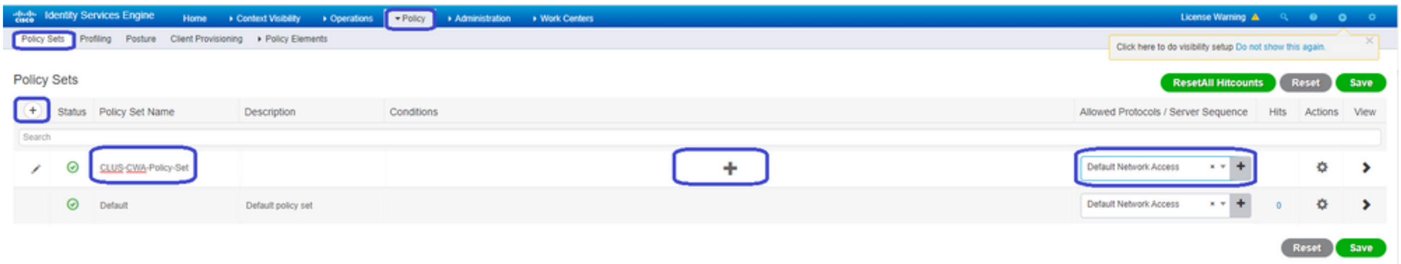
□ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth ACL CLUS-ACL Value Self-Registered Guest Portal (

CWAMABIDSSID

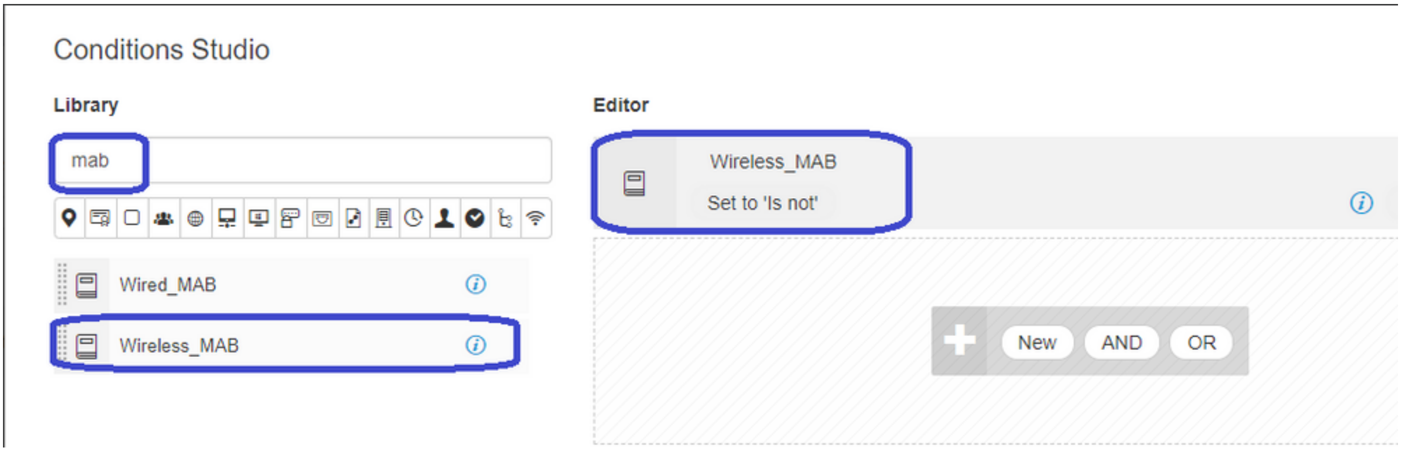
Policy>Policy Sets+MABPolicy>Policy Elements>Results>Authentication>Allowed Protocols +



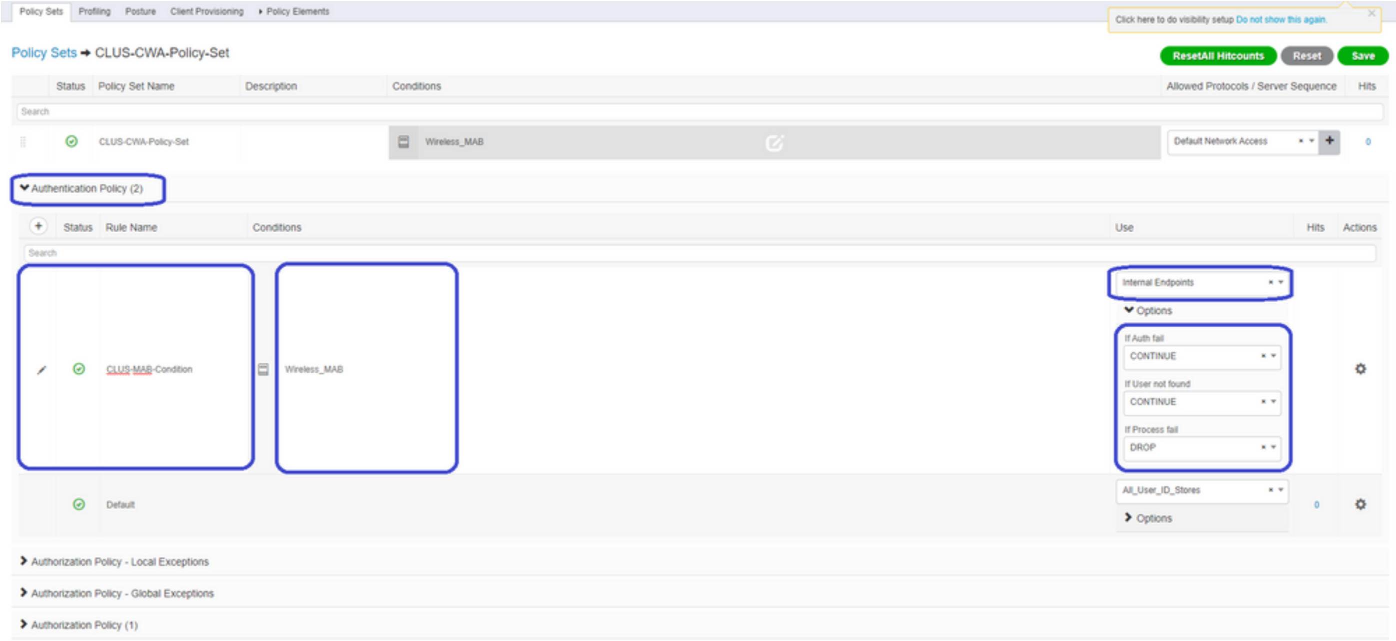
Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	CLUS-CWA-Policy-Set		+	Default Network Access		⚙	>
✓	Default	Default policy set		Default Network Access	0	⚙	>

ISEMABIDWLAN


Conditions Studio

MABID



Policy Sets → CLUS-CWA-Policy-Set

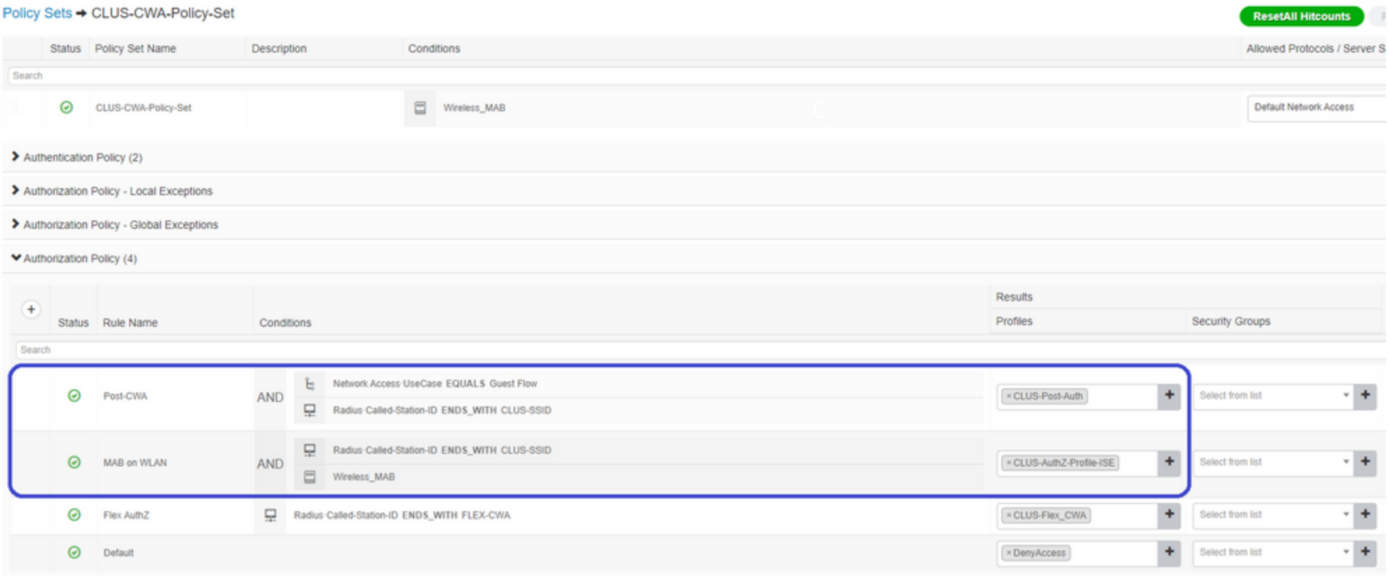
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access	0

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	CLUS-MAB-Condition	Wireless_MAB	Internal Endpoints Options If Auth fail: CONTINUE If User not found: CONTINUE If Process fail: DROP		⚙
✓	Default		All_User_ID_Stores Options	0	⚙

Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (1)

ACLpost-authpre-authSSIDIDWLAN



Policy Sets → CLUS-CWA-Policy-Set

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

> Authentication Policy (2)

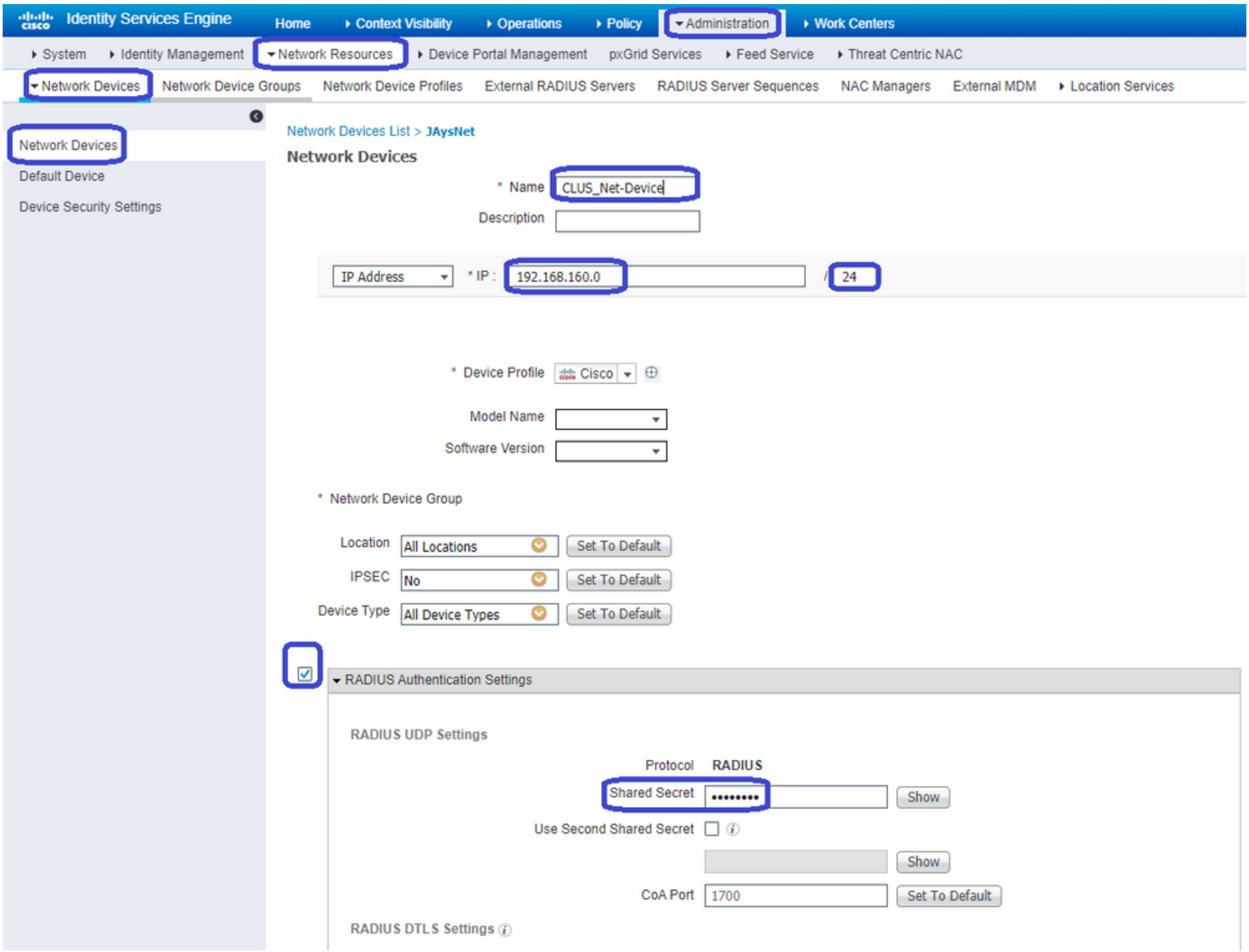
> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

⌄ Authorization Policy (4)

Status	Rule Name	Conditions	Results Profiles	Security Groups
✓	Post-CWA	AND Network Access-UseCase EQUALS Guest Flow Radius-Called-Station-ID ENDS_WITH CLUS-SSID	× CLUS-Post-Auth	Select from list
✓	MAB on WLAN	AND Radius-Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	× CLUS-AuthZ-Profile-ISE	Select from list
✓	Flex AuthZ	Radius-Called-Station-ID ENDS_WITH FLEX-CWA	× CLUS-Flex_CWA	Select from list
✓	Default		× DenyAccess	Select from list

ISE9800ISE**Admin>Network Resources>Network Device>**+.IPRADIUSISE9800



Network Devices List > JAysNet

Network Devices

* Name: CLUS_Net-Device

Description:

IP Address ▾ * IP : 192.168.160.0 / 24

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: •••••••• — Show

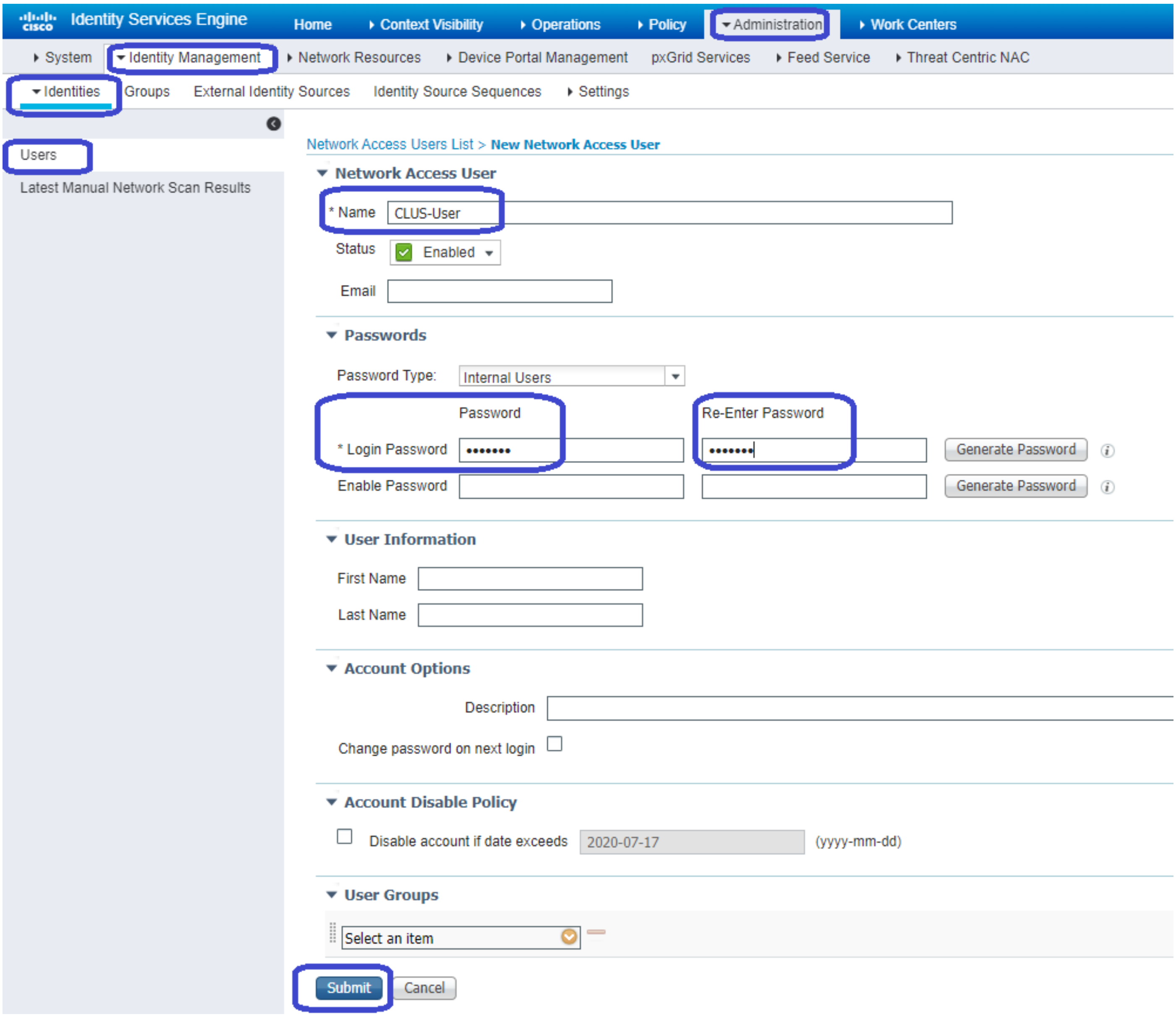
Use Second Shared Secret: □

Show

CoA Port: 1700 — Set To Default

RADIUS DTLS Settings

Admin>Identity Management>Identity>Users>+Add ISE



Network Access User

* Name: CLUS-User

Status: ☑ Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	•••••••	•••••••
Enable Password		

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

Account Disable Policy

□ Disable account if date exceeds 2020-07-17 (yyyy-mm-dd)

User Groups

Select an item

當AireOS WLC是外部，Catalyst 9800是錨點時，配置的差異

如果您希望AireOs WLC成為外部控制器，則配置與之前相同，只有兩個差異。

1. AAA記帳從來不在錨點上完成，因此9800沒有記帳方法清單，而AireOS WLC將啟用記帳並指向ISE。
2. AireOS需要錨定到9800而不是其自身。在策略配置檔案中，9800不會選擇錨點，但會選中「匯出錨點」框。
3. 必須注意的是，當AireOS WLC將使用者端匯出到9800時，並沒有原則設定檔的概念，只會傳送WLAN設定檔名稱。因此，9800會將從AireOS傳送的WLAN配置檔名稱應用到WLAN配置檔名稱和策略配置檔名稱。這表示從AireOS WLC錨定到9800 WLC時，兩個WLC上的WLAN設定檔名稱和9800上的原則設定檔名稱必須全部相符。

驗證

若要驗證9800 WLC上的**組態**，請執行命令

- AAA

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- 策略配置檔案

```
Show wireless profile policy detailed <profile name>
```

- 策略標籤

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- 驗證使用錨點的移動性是否啟動

```
Show wireless mobility summary
```

要驗證AireOS WLC上的配置，請運行命令

- AAA

```
Show radius summary
```

附註：RFC3576是CoA配置

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- 驗證與外部裝置的移動性是否正常

```
Show mobility summary
```

疑難排解

根據客戶端在該過程中停止的點，故障排除看起來不同。例如，如果WLC從未從MAB上的ISE收到響應，則客戶端將停滯在「Policy Manager State：（策略管理器狀態：）」Associating」和「 」將不會匯出到錨點。在這種情況下，您只會對外來路由器進行疑難排解，可能會為WLC和ISE之間的流量收集RA追蹤和封包擷取。另一個範例是MAB已成功通過，但使用者端沒有收到重新導向。在這種情況下，您需要確保外部在AVP中收到重定向並將其應用於客戶端。您還需要檢查錨點，以確保客戶端的正確ACL位於錨點上。 此故障排除範圍超出本技術文檔的設計範圍（有關通用客戶端故障排除指南的參考）。

如需更多有關在9800 WLC上排除CWA的幫助，請參閱Cisco Live!演示DGTL-TSCENT-404

Catalyst 9800故障排除資訊

客戶端詳細資訊

```
show wireless client mac-address
```

在此您應檢視「策略管理器狀態」、「會話管理器>身份驗證方法」、「移動角色」。

也可在GUI的「監控」(Monitoring)>「客戶端」(Clients)下找到此資訊

內嵌式封包擷取

在CLI中，命令啟動*#monitor capture <capture name>，然後*選項會在此後顯示。

在GUI上前往疑難排解>封包擷取>+Add

RadioActive跟蹤

在CLI上

```
debug wireless mac|ip
```

使用該命令的no形式將其停止。此檔案將記錄到bootflash中名為"ra_trace"的檔案中，然後記錄客戶端的MAC或IP地址以及日期和時間。

在GUI上，轉到「Troubleshoot」>「Radiative Trace」>「Add」。新增客戶端的mac或ip地址，點選apply，然後點選start。完成該過程數次後，停止跟蹤、生成日誌並將其下載到您的裝置。

AireOS故障排除資訊

客戶端詳細資訊

在CLI上*show client details <client mac>*

在GUI監視器>客戶端上

從CLI調試

```
Debug client

Debug mobility handoff

Debug mobility config
```

參考資料

[使用9800控制器構建移動隧道]()

9800上的無線調試和日誌收集